(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第7204231号
(P7204231)
(45)発行日　令和5年1月16日(2023.1.16)　(24)登録日　令和5年1月5日(2023.1.5)

(51)Int.Cl.　　F I
G06Q 20/02 (2012.01)　G06Q 20/02
G06Q 20/10 (2012.01)　G06Q 20/10

請求項の数 40　外国語出願　(全 78 頁)

(21)出願番号　特願2020-209670(P2020-209670)
(22)出願日　令和2年12月17日(2020.12.17)
(62)分割の表示　特願2017-511157(P2017-511157)の分割
原出願日　平成27年5月5日(2015.5.5)
(65)公開番号　特開2021-61021(P2021-61021A)
(43)公開日　令和3年4月15日(2021.4.15)
審査請求日　令和3年1月15日(2021.1.15)
(31)優先権主張番号　61/990,795
(32)優先日　平成26年5月9日(2014.5.9)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　516335038
ミドルトン，レジナルド
アメリカ合衆国，エヌワイ　１１２１８，ブルックリン，１９５　アーガイル　アールディー
(74)代理人　110002952
弁理士法人鷲田国際特許事務所
(72)発明者　ミドルトン，レジナルド
アメリカ合衆国，エヌワイ　１１２１８，ブルックリン，１９５　アーガイル　アールディー
(72)発明者　ボゴシアン，マシュー
アメリカ合衆国，ダブリューエー　９８２２１，アナコルテス，５００７　トータム　ティーアールエル

最終頁に続く

(54)【発明の名称】信頼度が低い、または信頼度が皆無の当事者間での価値転送を円滑化する装置、システム、または方法

(57)【特許請求の範囲】

【請求項１】

転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を円滑化するシステムであって、前記転送メカニズムは、ファシリテータ、前記第一のクライアント、および第二のクライアントによってそれぞれコンピュータネットワークを介してアクセス可能な分散型デジタル通貨を含み、前記システムは、前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントを含み、

ａ．前記ファシリテータは、

ｉ．取引記録セクタと第一の非対称キーペアを保管する第一のキーペアセクタとを有する第一のメモリであって、前記第一の非対称キーペアは、第一のプライベートキーおよび第一のパブリックキーを有する、第一のメモリと、

ｉｉ．支払額を決定するために使用する条件を受け取る第一のネットワークインターフェースであって、前記条件は、

Ａ．第一の元本額および第二の元本額の少なくとも１つと、

Ｂ．第一のデータソースおよび第二のデータソースの少なくとも１つへの参照であって、前記第一のデータソースは、第一の証券に関するデータを保管する第一のデータベースを含み、前記第二のデータソースは、第二の証券に関するデータを保管する第二のデータベースを有する、前記参照と、

Ｃ．支払条件と、

Ｄ．有効期限タイムスタンプと、を含む、第一のネットワークインターフェースと、を含み、
ｂ．前記第一のクライアントは、
ｉ．第二の非対称キーペアを保管する第二のキーペアセクタを有する第二のメモリであって、前記第二の非対称キーペアは、第二のプライベートキーおよび第二のパブリックキーを有する、第二のメモリと、
ｉｉ．第二のネットワークインターフェースと、
ｉｉｉ．前記第二のメモリおよび前記第二のネットワークインターフェースに結合された第二のコンピュータプロセッサであって、
Ａ．前記第二のキーペアセクタから前記第二のプライベートキーを読み取り、
Ｂ．前記第二のプライベートキーを使用して第一のソース取引記録を作成し、署名し、
Ｃ．未完了のコミット取引記録を作成し、前記未完了のコミット取引記録は、
Ｉ．前記第一のデータソースおよび前記第二のデータソースの少なくとも１つからの値と、
ＩＩ．コミット額と、
ＩＩＩ．前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントの少なくとも２つの承認を必要とする条件と、
を含み、
Ｄ．前記第二のプライベートキーを使用して前記未完了のコミット取引記録に署名することによって完全なコミット取引記録を作成し、
Ｅ．未完了の有効期限取引記録を作成し、前記未完了の有効期限取引記録は、
Ｉ．前記有効期限タイムスタンプ以降のロックタイムと、
ＩＩ．前記コミット額と、
ＩＩＩ．第一の有効期限額と、前記第一のクライアントの承認を必要とする第一の条件とを含む、第一の有効期限出力と、を含み、
Ｆ．前記第二のプライベートキーを使用して前記未完了の有効期限取引記録に署名し、
Ｇ．前記完全なコミット取引記録および前記未完了の有効期限取引記録を前記第二のクライアントへ送信し、
ｃ．前記第二のクライアントは、
ｉ．第三の非対称キーペアを保管する第三のキーペアセクタを有する第三のメモリであって、前記第三の非対称キーペアは、第三のプライベートキーおよび第三のパブリックキーを有する、第三のメモリと、
ｉｉ．第三のネットワークインターフェースと、
ｉｉｉ．前記第三のメモリおよび前記第三のネットワークインターフェースに結合された第三のコンピュータプロセッサであって、
Ａ．前記未完了の有効期限取引記録を読み取り、
Ｂ．前記第三のキーペアセクタから前記第三のプライベートキーを読み取り、
Ｃ．前記第三のプライベートキーを使用して前記未完了の有効期限取引記録に署名することによって、完全な有効期限取引記録を作成し、
Ｄ．前記完全な有効期限取引記録を前記第一のクライアントへ送信する、ように構成され、
前記ファシリテータの第一のコンピュータプロセッサは、
Ａ．アプリケーションプログラムインターフェース（ＡＰＩ）を介して、前記第一のデータソースおよび前記第二のデータソースの少なくとも１つから前記支払条件を満たすことを検出すると、支払機能を以下に適用して、一つ以上の支払額を計算し、
Ｉ．前記第一の元本額および前記第二の元本額の少なくとも１つと、
ＩＩ．前記第一のデータソースおよび前記第二のデータソースの少なくとも１つからの前記値と、

Ｂ．前記第一のキーペアセクタから前記第一のプライベートキーを読み取り、
Ｃ．前記第一のプライベートキーを使用して未完了の支払取引記録を作成し、署名し、前記未完了の支払取引は、
Ｉ．前記コミット取引から受け取った前記コミット額と、
ＩＩ．前記一つ以上の支払額と、
を含み、
Ｄ．前記署名された未完了の支払取引記録を前記第一のクライアントと前記第二のクライアントに発行することによって、前記第一のクライアントと前記第二のクライアントの少なくとも１つが、完全な支払取引記録を作成する、ように構成され、
前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントは、前記第一のネットワークインターフェース、前記第二のネットワークインターフェース、および前記第三のネットワークインターフェースをそれぞれ介して、前記コンピュータネットワークに結合されている、システム。
【請求項２】
前記支払条件は、
ｉ．前記第一のデータソースおよび前記第二のデータソースの少なくとも１つに対する質問からの結果と、
ｉｉ．予想される場所におけるデータの有無の観察と、
ｉｉｉ．予想される値の組の中または予想されパターンに一致するかどうかの決定と、
ｉｖ．デジタル機器からの信号を受信し、信号値が予想される範囲または許容値内であることを検証することと、
を含む、請求項１に記載のシステム。
【請求項３】
前記第三のコンピュータプロセッサが、第二のソース取引記録を作成し、署名し、前記第二のソース取引記録を前記転送メカニズムに提出することによって、前記第二のソース取引を有効にするようにさらに構成される、請求項１に記載のシステム。
【請求項４】
前記第二のコンピュータプロセッサは、前記第二のメモリ中に前記完全なコミット取引記録を保管するように、さらに構成され、
前記第三のコンピュータプロセッサは、前記第三のメモリ中に前記完全なコミット取引記録を保管し、前記第三のメモリ中に前記完全な有効期限取引記録を保管するように、さらに構成された、請求項１に記載のシステム。
【請求項５】
前記未完了の有効期限取引記録は、第二の有効期限額および前記第二のクライアントの承認を必要とする条件と、を含む第二の有効期限出力を、さらに含む、請求項１に記載のシステム。
【請求項６】
前記一つ以上の支払額は、
ｉ．第一の支払額と前記第二のクライアントの承認を必要とする条件と、
ｉｉ．第二の支払額と前記第一のクライアントの承認を必要とする条件と、
ｉｉｉ．手数料額と第三者の承認を必要とする条件と、
のうち少なくとも１つを含む、請求項１に記載のシステム。
【請求項７】
前記第一のコンピュータプロセッサは、
ａ．前記第一のプライベートキーを使用して、未完了の払い戻し取引記録を作成し、署名することであって、前記未完了の払い戻し取引記録は、
ｉ．前記コミット取引から受け取った前記コミット額と、
ｉｉ．払い戻し額と、
を含み、

ｂ．前記未完了の払い戻し取引記録を前記第一のクライアントおよび前記第二のクライアントの少なくとも１つに発行する、
ようにさらに構成され、
前記第二のコンピュータプロセッサまたは前記第三のコンピュータプロセッサは、
前記未完了の払い戻し取引記録から完全な払い戻し取引記録を作成し、前記完全な払い戻し取引記録は、前記第一のクライアントまたは前記第二のクライアントが完全に失敗した事象が発生した場合でも資金を回収することができるように払い戻し取引を作成するために使用される、請求項１に記載のシステム。
【請求項８】
転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を円滑化する方法であって、前記転送メカニズムは、ファシリテータ、前記第一のクライアント、および第二のクライアントによってそれぞれコンピュータネットワークを介してアクセス可能な分散型デジタル通貨を含み、前記方法は、
ａ．第一の非対称キーペアを前記ファシリテータによって保管することであって、前記第一の非対称キーペアは、第一のプライベートキーおよび第一のパブリックキーを含み、
ｂ．支払額を決定するための条件を前記ファシリテータによって受け取ることであって、前記条件は、
Ａ．第一の元本額および第二の元本額の少なくとも１つと、
Ｂ．第一のデータソースおよび第二のデータソースの少なくとも１つへの参照であって、前記第一のデータソースは、第一の証券に関するデータを保管する第一のデータベースを含み、前記第二のデータソースは、第二の証券に関するデータを保管する第二のデータベースを有する、前記参照と、
Ｃ．支払条件と、
Ｄ．有効期限タイムスタンプと、を含み、
ｃ．前記第一のクライアントによって、第二の非対称キーペアを保管することであって、前記第二の非対称キーペアは、第二のプライベートキーおよび第二のパブリックキーを有し、
ｄ．前記第一のクライアントによって、第二のキーペアセクタから前記第二のプライベートキーを読み取ることと、
ｅ．前記第一のクライアントによって、前記第二のプライベートキーを使用して第一のソース取引記録を作成し、署名することと、
ｆ．前記第一のクライアントによって、以下を含む未完了のコミット取引記録を作成することと、
Ｉ．前記第一のデータソースおよび前記第二のデータソースの少なくとも１つからの値と、
ＩＩ．コミット額と、
ＩＩＩ．前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントの少なくとも２つの承認を必要とする条件と、
ｇ．前記第一のクライアントによって、前記第二のプライベートキーを使用して前記未完了のコミット取引記録に署名することと、
ｈ．以下を含む未完了の有効期限取引記録を作成することと、
Ｉ．前記有効期限タイムスタンプ以降のロックタイムと、
ＩＩ．コミット額と、
ＩＩＩ．前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントの少なくとも２つの承認を必要とする条件と、
ｉ．前記第二のプライベートキーを使用して前記未完了の有効期限取引記録に署名することと、
ｊ．完全なコミット取引記録および前記未完了の有効期限取引記録を前記第二のクライアントへ送信することと、

ｋ．前記第二のクライアントによって、第三の非対称キーペアを保管することであって、前記第三の非対称キーペアは、第三のプライベートキーおよび第三のパブリックキーを有し、
ｌ．前記第二のクライアントによって、前記未完了の有効期限取引記録を読み取ることと、
ｍ．前記第二のクライアントによって、第三のキーペアセクタから前記第三のプライベートキーを読み取ることと、
ｎ．前記第二のクライアントによって、前記第三のプライベートキーを使用して前記未完了の有効期限取引記録に署名することによって、完全な有効期限取引記録を作成することと、
ｏ．前記第二のクライアントによって、前記完全な有効期限取引記録を前記第一のクライアントへ送信することと、
ｐ．前記第一のクライアントによって、第一のソース取引記録を前記転送メカニズムに送り、前記第一のソース取引を有効にすることと、
ｑ．前記第一のクライアントによって、前記完全なコミット取引記録を前記転送メカニズムに送り、前記コミット取引を有効にすることと、
ｒ．前記ファシリテータによって、アプリケーションプログラムインターフェース（ＡＰＩ）を介して、前記第一のデータソースおよび前記第二のデータソースの少なくとも１つから前記支払条件を満たすことを検出すると、支払機能を以下に適用して、一つ以上の支払額を計算することと、
Ｉ．前記第一の元本額および前記第二の元本額の少なくとも１つと、
ＩＩ．前記第一のデータソースおよび前記第二のデータソースの少なくとも１つからの前記値と、
ｓ．前記ファシリテータによって、第一のキーペアセクタから前記第一のプライベートキーを読み取ることと、
ｔ．前記ファシリテータによって、前記第一のプライベートキーを使用して、以下を含む未完了の支払取引記録を作成し、署名することと、
Ｉ．前記コミット取引から受け取った前記コミット額と、
ＩＩ．前記一つ以上の支払額と、
ｕ．前記ファシリテータによって、前記署名された未完了の支払取引記録を前記第一のクライアントと前記第二のクライアントに発行することによって、前記第一のクライアントと前記第二のクライアントの少なくとも１つが、完全な支払取引記録を作成することと、
を含み、
前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントは、第一のネットワークインターフェース、第二のネットワークインターフェース、および第三のネットワークインターフェースをそれぞれ介して、前記コンピュータネットワークに結合されている、方法。
【請求項９】
前記支払条件は、
ｉ．前記第一のデータソースおよび前記第二のデータソースの少なくとも１つに対する質問からの結果と、
ｉｉ．予想される場所におけるデータの有無の観察と、
ｉｉｉ．予想される値の組の中または予想されパターンに一致するかどうかの決定と、
ｉｖ．デジタル機器からの信号を受信し、信号値が予想される範囲または許容値内であることを検証すること、
を含む、請求項８に記載の方法。
【請求項１０】
前記第二のクライアントによって、第二のソース取引記録を作成し、署名し、

前記第二のクライアントによって、前記第二のソース取引記録を前記転送メカニズムに提出することによって、前記第二のソース取引を有効にすることを、さらに含む、請求項８に記載の方法。

【請求項１１】

前記第一のクライアントによって、前記第二のメモリ中に前記完全なコミット取引を保管し、

前記第二のクライアントによって、前記第三のメモリ中に前記完全なコミット取引を保管し、前記第三のメモリ中に前記完全な有効期限取引記録を保管することを、さらに含む、請求項８に記載の方法。

【請求項１２】

前記未完了の有効期限取引記録は、第二の有効期限額および前記第二のクライアントの承認を必要とする条件を含む第二の有効期限出力を、さらに含む、請求項８に記載の方法。

【請求項１３】

前記二つ以上の支払額は、

ｉ．第一の支払額と前記第二のクライアントの承認を必要とする条件と

ｉｉ．第二の支払額と前記第一のクライアントの承認を必要とする条件と

ｉｉｉ．手数料額、および第三者の承認を必要とする条件と、

のうち少なくとも１つを含む、請求項８に記載の方法。

【請求項１４】

前記方法は、

ａ．前記第一のプライベートキーを使用して、未完了の払い戻し取引記録を作成し、署名し、前記未完了の払い戻し取引記録は、

ｉ．前記コミット取引から受け取った前記コミット額と、

ｉｉ．払い戻し額と、を含み、

ｂ．前記未完了の払い戻し取引記録を前記第一のクライアントおよび第二のクライアントの少なくとも１つに発行し、

ｃ．前記未完了の払い戻し取引記録から完全な払い戻し取引記録を作成し、前記完全な払い戻し取引記録は、前記第一のクライアントまたは前記第二のクライアントが完全に失敗した事象が発生した場合でも資金を回収することができるように払い戻し取引を作成するために使用される、

を含む、請求項８に記載の方法。

【請求項１５】

転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を円滑化するシステムであって、前記転送メカニズムは、ファシリテータ、前記第一のクライアント、および第二のクライアントによってそれぞれコンピュータネットワークを介してアクセス可能な分散型デジタル通貨を含み、前記システムは、前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントを含み、

ａ．前記ファシリテータは、

ｉ．取引記録セクタと第一の非対称キーペアを保管する第一のキーペアセクタとを有する第一のメモリであって、前記第一の非対称キーペアは、第一のプライベートキーおよび第一のパブリックキーを有する、第一のメモリと、

ｉｉ．支払額を決定するための条件を受け取る第一のネットワークインターフェースであって、前記条件は、

Ａ．第一の元本額および第二の元本額の少なくとも１つと、

Ｂ．第一のデータソースおよび第二のデータソースの少なくとも１つへの参照と、

前記第一のデータソースは、第一の証券に関するデータを保管する第一のデータベースを含み、前記第二のデータソースは、第二の証券に関するデータを保管する第二のデータベースを有する、

を含む、第一のネットワークインターフェースと、
ｉｉｉ．前記第一のメモリおよび前記第一のネットワークインターフェースに結合された第一のコンピュータプロセッサであって、
Ａ．支払機能を、
前記第一の元本額および前記第二の元本額の少なくとも１つ、および
前記第一のデータソースおよび前記第二のデータソースの少なくとも１つからの値に適用することにより、一つ以上の支払額を計算し、
Ｂ．前記第一のキーペアセクタから前記第一のプライベートキーを読み取り、
Ｃ．前記第一のプライベートキーから第一の暗号署名を計算し、
Ｄ．未完了の支払取引記録を作成し、前記未完了の支払取引記録は、
Ｉ．コミット取引から受け取るコミット額
ＩＩ．前記一つ以上の支払額、および
ＩＩＩ．前記第一の暗号署名、を含む、
Ｅ．前記未完了の支払取引記録を前記第一のクライアントまたは前記第二のクライアントの少なくとも１つに発行する、第一のコンピュータプロセッサと、
を含み、
ｂ．前記第一のクライアントは、
ｉ．第二の非対称キーペアを保管する第二のキーペアセクタを有する第二のメモリであって、前記第二の非対称キーペアは、第二のプライベートキーおよび第二のパブリックキーを有する、第二のメモリと、
ｉｉ．第二のネットワークインターフェースと、
ｉｉｉ．前記第二のメモリおよび前記第二のネットワークインターフェースに結合された第二のコンピュータプロセッサであって、
Ａ．前記第二のキーペアセクタから前記第二のプライベートキーを読み取り、
Ｂ．前記未完了の支払取引記録を読み取り、
Ｃ．前記第二のプライベートキーから第二の暗号署名を計算し、
Ｄ．完了した支払取引記録を作成し、前記完了した支払取引記録は、
Ｉ．前記コミット額、
ＩＩ．前記一つ以上の支払額、
ＩＩＩ．前記第一の暗号署名、および
ＩＶ．前記第二の暗号署名、を含む、
Ｅ．前記完了した支払取引記録を前記転送メカニズムに提出することにより支払取引を作成する、第二のコンピュータプロセッサと、
を含み、
ｃ．前記第二のクライアントは、
ｉ．第三の非対称キーペアを保管する第三のキーペアセクタを有する第三のメモリであって、前記第三の非対称キーペアは、第三のプライベートキーおよび第三のパブリックキーを有する、第三のメモリと、
ｉｉ．第三のネットワークインターフェースと、
ｉｉｉ．前記第三のメモリおよび前記第三のネットワークインターフェースに結合された第三のコンピュータプロセッサであって、前記第三のキーペアセクタから前記第三のプライベートキーを読み取る、第三のコンピュータプロセッサと、を含み、
前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントは、前記第一のネットワークインターフェース、前記第二のネットワークインターフェース、および前記第三のネットワークインターフェースをそれぞれ介して前記コンピュータネットワークに結合されている、
システム。
【請求項１６】
前記第一のコンピュータプロセッサは、
ａ．前記第一のプライベートキーから第三の暗号署名を作成し、

ｂ．以下を有する未完了の払い戻し取引記録を作成し、
ｉ．前記コミット取引から受け取った前記コミット額と、
ｉｉ．払い戻し額と、
ｉｉｉ．前記第三の暗号署名と、
ｃ．前記未完了の払い戻し取引記録を前記第一のクライアントまたは前記第二のクライアントの少なくとも１つに発行する、
ようにさらに構成され、
前記第二のコンピュータプロセッサまたは第三のコンピュータプロセッサは、前記未完了の払い戻し取引記録から完全な払い戻し取引記録を作成するようにさらに構成され、前記完全な払い戻し取引記録は、前記第一のクライアントまたは前記第二のクライアントが、完全に失敗した事象が発生した場合でも資金を回収できるにより払い戻し取引を作成するために使用される、請求項１５に記載のシステム。
【請求項１７】
転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を、円滑化するシステムによって実行される方法であって、前記転送メカニズムが、ファシリテータ、前記第一のクライアント、および第二のクライアントによってそれぞれコンピュータネットワークを介してアクセス可能な分散型デジタル通貨を含む、方法であって、
ａ．前記第一のクライアントが、第一の非対称キーペアを第一のメモリの第一のキーペアセクタに保管するステップであって、前記第一の非対称キーペアは、第一のパブリックキーおよび第一のプライベートキーを有する、ステップと、
ｂ．前記ファシリテータが、第二の非対称キーペアを第二のメモリの第二のキーペアセクタに保管するステップであって、前記第二の非対称キーペアは、第二のパブリックキーおよび第二のプライベートキーを有する、ステップと、
ｃ．前記ファシリテータが、第三の非対称キーペアを前記第二のキーペアセクタに保管するステップであって、前記第三の非対称キーペアは、第三のパブリックキーおよび第三のプライベートキーを有する、ステップと、
ｄ．前記第一のクライアントが、第四の非対称キーペアを第三のメモリの第三のキーペアセクタに保管するステップであって、前記第四の非対称キーペアは、第四のパブリックキーおよび第四のプライベートキーを有する、ステップと、
ｅ．前記第一のクライアントが、ネットワークインターフェースを介して支払額を決定するための条件を送信するステップであって、前記条件は、
ｉ．第一の元本額および第二の元本額の少なくとも１つと、
ｉｉ．第一のデータソースおよび第二のデータソースの少なくとも１つへの参照と、
前記第一のデータソースは、証券に関するデータを保管する第一のデータベースを含み、
前記第二のデータソースは、第二の証券に関するデータを保管する第二のデータベースを有する、
を含む、ステップと、
ｆ．前記ファシリテータが、前記条件を第二のネットワークインターフェースを介して受け取るステップと、
ｇ．前記ファシリテータが、支払機能を、
ｉ．前記第一の元本額および前記第二の元本額の少なくとも１つ、および
ｉｉ．前記第一のデータソースおよび前記第二のデータソースの少なくとも１つからの値、に適用することにより、一つ以上の支払額を計算するステップと、
ｈ．前記第一のクライアントが、前記第一のキーペアセクタから前記第一のプライベートキーを読み取るステップと、
ｉ．前記ファシリテータが、前記第一のプライベートキーから第一の暗号署名を計算するステップと、
ｊ．前記第一のクライアントが、第一の元本取引記録を作成するステップであって、前記第一の元本取引記録は、

ｉ．前記第一の元本額、および
ｉｉ．前記第一の暗号署名、を含む、ステップと、
ｋ．前記第一のクライアントが、前記第一の元本取引記録を前記転送メカニズムに提出することにより第一の元本取引を作成するステップと、
ｌ．前記ファシリテータが、前記第二のキーペアセクタから前記第二のプライベートキーを読み取るステップと、
ｍ．前記ファシリテータが、前記第二のプライベートキーから第二の暗号署名を計算するステップと、
ｎ．前記ファシリテータが、コミット取引記録を作成するステップであって、前記コミット取引記録は、
ｉ．前記第一の元本額、
ｉｉ．コミット額、および
ｉｉｉ．前記第二の暗号署名、を含む、ステップと、
ｏ．前記ファシリテータが、前記コミット取引記録を前記転送メカニズムに提出することによりコミット取引を作成するステップと、
ｐ．前記ファシリテータが、前記第一のデータソースから前記証券の値を引き出すステップと、
ｑ．前記ファシリテータが、前記第二のキーペアセクタから前記第三のプライベートキーを読み取るステップと、
ｒ．前記ファシリテータが、前記第二のプライベートキーから第三の暗号署名を計算するステップと、
ｓ．前記ファシリテータが、未完了の支払取引記録を作成するステップであって、前記未完了の支払取引記録は、
ｉ．前記コミット取引から受け取る前記コミット額、
ｉｉ．前記一つ以上の支払額、および
ｉｉｉ．前記第三の暗号署名、を含む、ステップと、
ｔ．前記ファシリテータが、前記未完了の支払取引記録を前記第一のクライアントまたは前記第二のクライアントの少なくとも１つに発行するステップと、
ｕ．前記第一のクライアントが、前記未完了の支払取引記録を読み取るステップと、
ｖ．前記第一のクライアントが、前記第三のキーペアセクタから前記第四のプライベートキーを読み取るステップと、
ｗ．前記第一のクライアントが、前記第四のプライベートキーから第四の暗号署名を計算するステップと、
ｘ．前記第一のクライアントが、完了した支払取引記録を作成するステップであって、前記完了した支払取引記録は、
ｉ．前記コミット額、
ｉｉ．前記一つ以上の支払額、
ｉｉｉ．前記第三の暗号署名、および
ｉｖ．前記第四の暗号署名、を含む、ステップと、
ｙ．前記第一のクライアントが、前記完了した支払取引記録を前記転送メカニズムに提出することにより支払取引を作成するステップと、
を有する、方法。
【請求項１８】
前記方法は、
ａ．前記ファシリテータによって、前記第一のプライベートキーから第三の暗号署名を計算することと、
ｂ．以下を有する未完了の払い戻し取引記録を作成することと、
ｉ．前記コミット取引から受け取った前記コミット額と、
ｉｉ．払い戻し額と、
ｉｉｉ．前記第三の暗号署名と、

ｃ．前記未完了の払い戻し取引記録を前記第一のクライアントおよび前記第二のクライアントの少なくとも１つに発行することと、
ｄ．前記未完了の払い戻し取引記録から完全な払い戻し取引記録を作成することであって、前記完全な払い戻し取引記録は、前記第一のクライアントまたは前記第二のクライアントが、完全に失敗した事象が発生した場合でも資金を回収できるにより払い戻し取引を作成するために使用される、
をさらに含む、請求項１７に記載の方法。
【請求項１９】
前記条件は、有効期限タイムスタンプをさらに含み、前記有効期限タイムスタンプは、いつ前記条件が失効するかを示す日時によって指定されか、または前記有効期限タイムスタンプは、前記条件が失効しないことを示す無限に設定される、請求項１７に記載の方法。
【請求項２０】
転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を円滑化する装置であって、前記転送メカニズムが、前記装置、前記第一のクライアント、および第二のクライアントによってそれぞれコンピュータネットワークを介してアクセス可能な分散型デジタル通貨を含む、装置であって、
ａ．取引記録セクタと第一の非対称キーペアを保管する第一のキーペアセクタとを有する第一のメモリであって、前記第一の非対称キーペアは、第一のプライベートキーおよび第一のパブリックキーを有する、第一のメモリと、
ｂ．支払額を決定するための条件を受け取る第一のネットワークインターフェースであって、前記条件は、
ｉ．第一の元本額および第二の元本額の少なくとも１つと、
ｉｉ．第一のデータソースおよび第二のデータソースの少なくとも１つへの参照と、前記第一のデータソースは、第一の証券に関するデータを保管する第一のデータベースを有し、前記第二のデータソースは、第二の証券に関するデータを保管する第二のデータベースを有する、を含む、第一のネットワークインターフェースと、
ｃ．前記第一のメモリおよび前記第一のネットワークインターフェースに結合された第一のコンピュータプロセッサであって、
ｉ．支払機能を、
Ａ．前記第一の元本額および前記第二の元本額の少なくとも１つ、および
Ｂ．前記第一のデータソースおよび前記第二のデータソースの少なくとも１つからの値、に適用することにより、一つ以上の支払額を計算し、
ｉｉ．前記第一のキーペアセクタから前記第一のプライベートキーを読み取り、
ｉｉｉ．前記第一のプライベートキーから第一の暗号署名を計算し、
ｉｖ．未完了の支払取引記録を作成し、前記未完了の支払取引記録は、
Ａ．コミット取引から受け取るコミット額、
Ｂ．前記一つ以上の支払額、および
Ｃ．前記第一の暗号署名、を含む、
ｖ．前記未完了の支払取引記録を前記第一のクライアントおよび前記第二のクライアントの少なくとも１つに発行する、第一のコンピュータプロセッサと、
を有し、
前記装置、前記第一のクライアント、および前記第二のクライアントは、前記第一のネットワークインターフェース、第二のネットワークインターフェース、および第三のネットワークインターフェースをそれぞれ介して前記コンピュータネットワークに結合されており、
前記未完了の支払取引記録は、完全な支払取引記録を前記転送メカニズムに送ることによって完全な支払取引を作成するために前記第一のクライアントおよび前記第二のクライアントの少なくとも１つによって使用され、

前記完全な支払取引記録は、
Ａ．前記コミット額と、
Ｂ．前記一つ以上の支払額と、
Ｃ．前記第一の暗号署名と、
Ｄ．前記第一のクライアントに保管された第二のプライベートキーから計算された第二の暗号署名と、含む、装置。
【請求項２１】
前記第一のコンピュータプロセッサは、
ａ．前記第一のプライベートキーから第三の暗号署名を計算し、
ｂ．以下を含む未完了の払い戻し取引記録を作成し、
ｉ．前記コミット取引から受け取った前記コミット額と、
ｉｉ．払い戻し額と、
ｉｉｉ．前記第三の暗号署名と、
ｉｖ．ロックタイムと、
ｃ．前記未完了の払い戻し取引記録を前記第一のクライアントまたは前記第二のクライアントの少なくとも１つに発行する、
ようにさらに構成され、
前記未完了の払い戻し取引記録は、前記第一のクライアントおよび／または前記第二のクライアントが、完全に失敗した事象が発生した場合でも資金を回収できるように払い戻し取引を作成することに使用される、請求項２０に記載の装置。
【請求項２２】
前記条件は、有効期限タイムスタンプをさらに含み、前記有効期限タイムスタンプは、いつ前記条件が失効するかを示す日時によって指定されか、または前記有効期限タイムスタンプは、前記条件が失効しないことを示す無限に設定される、請求項２０に記載の装置。
【請求項２３】
転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を円滑化する装置であって、前記転送メカニズムが、前記装置、前記第一のクライアント、および第二のクライアントによってそれぞれコンピュータネットワークを介してアクセス可能な分散型デジタル通貨を含む、装置であって、
ａ．取引記録セクタと第一の非対称キーペアを記憶する第一のキーペアセクタとを有する第一のメモリであって、前記第一の非対称キーペアは、第一のプライベートキーおよび第一のパブリックキーを有する、第一のメモリと、
ｂ．支払額を決定するための条件を受け取る第一のネットワークインターフェースであって、前記条件は、
ｉ．第一の元本額および第二の元本額の少なくとも一方と、
ｉｉ．第一のデータソースおよび第二のデータソースの少なくとも一方への参照と、前記第一のデータソースは、第一の証券に関するデータを記憶する第一のデータベースを有し、前記第二のデータソースは、第二の証券に関するデータを記憶する第二のデータベースを有する、
ｉｉｉ．有効期限タイムスタンプと、を含む、第一のネットワークインターフェースと、
ｃ．前記第一のメモリおよび前記第一のネットワークインターフェースに結合された第一のコンピュータプロセッサであって、
ｉ．支払機能を、
Ａ．前記第一の元本額および前記第二の元本額の少なくとも一方、および
Ｂ．前記第一のデータソースおよび前記第二のデータソースの少なくとも一方からの値、に適用することにより、一つ以上の支払額を計算し、
ｉｉ．前記第一のキーペアセクタから前記第一のプライベートキーを読み取り、

ｉｉｉ．前記第一のプライベートキーから第一の暗号署名を計算し、
ｉｖ．未完了の支払取引記録を作成し、前記未完了の支払取引記録は、
Ａ．約定取引から受け取る約定額、
Ｂ．前記一つ以上の支払額、および
Ｃ．前記第一の暗号署名、を含む、
ｖ．前記未完了の支払取引記録を前記第一のクライアントおよび前記第二のクライアントの少なくとも一方に発行する、第一のコンピュータプロセッサと、
を有する、
ここで、前記第一のクライアントは、
ａ．第二の非対称キーペアを記憶する第二のキーペアセクタを有する第二のメモリであって、前記第二の非対称キーペアは、第二のプライベートキーおよび第二のパブリックキーを有する、第二のメモリと、
ｂ．第二のネットワークインターフェースと、
ｃ．前記第二のメモリおよび前記第二のネットワークインターフェースに結合された第二のコンピュータプロセッサであって、
ｉ．前記第二のキーペアセクタから前記第二のプライベートキーを読み取り、
ｉｉ．前記未完了の支払取引記録を読み取り、
ｉｉｉ．前記第二のプライベートキーから第二の暗号署名を計算し、
ｉｖ．完了した支払取引記録を作成し、前記完了した支払取引記録は、
Ａ．前記約定額、
Ｂ．前記一つ以上の支払額、
Ｃ．前記第一の暗号署名、および
Ｄ．前記第二の暗号署名、を含む、
ｖ．前記完了した支払取引記録を前記転送メカニズムに提出することにより支払取引を作成する、第二のコンピュータプロセッサと、を有し、
前記第二のクライアントは、
ａ．第三の非対称キーペアを記憶する第三のキーペアセクタを有する第三のメモリであって、前記第三の非対称キーペアは、第三のプライベートキーおよび第三のパブリックキーを有する、第三のメモリと、
ｂ．第三のネットワークインターフェースと、
ｃ．前記第三のメモリおよび前記第三のネットワークインターフェースに結合された第三のコンピュータプロセッサであって、前記第三のキーペアセクタから前記第三のプライベートキーを読み取る、第三のコンピュータプロセッサと、を有し、
前記装置、前記第一のクライアント、および前記第二のクライアントは、前記第一のネットワークインターフェース、前記第二のネットワークインターフェース、および前記第三のネットワークインターフェースをそれぞれ介して前記コンピュータネットワークに結合されており、
前記第一のコンピュータプロセッサは、更に、
ａ．前記第一のプライベートキーから第三の暗号署名を計算し、
ｂ．未完了の払戻取引記録を作成し、前記未完了の払戻取引記録は、
ｉ．前記約定取引から受け取る前記約定額、
ｉｉ．払戻額、
ｉｉｉ．前記第三の暗号署名、および
ｉｖ．ロックタイム、を含む、
ｃ．前記未完了の払戻取引記録を前記第一のクライアントまたは前記第二のクライアントの少なくとも一方に発行し、
ａ．前記第一のキーペアセクタは、更に、第四の非対称キーペアを記憶し、前記第四の非対称キーペアは、第四のプライベートキーおよび第四のパブリックキーを有する、
ｂ．前記第一のコンピュータプロセッサは、更に、
ｉ．前記第一のキーペアセクタから前記第四のプライベートキーを読み取り、

ｉｉ．前記第四のプライベートキーから第四の暗号署名を計算し、
ｉｉｉ．約定取引記録を作成し、前記約定取引記録は、
Ａ．前記第一の元本額、
Ｂ．前記約定額、および
Ｃ．前記第四の暗号署名、を含む、
ｉｖ．前記約定取引記録を前記転送メカニズムに提出することにより前記約定取引を作成し、
前記第一の非対称キーペアは、前記第四の非対称キーペアと同一であり、前記第一のプライベートキーは、前記第四のプライベートキーと同一であり、前記第一のパブリックキーは、前記第四のパブリックキーと同一であり、
ａ．前記第一のデータソースまたは前記第二のデータソースへの前記参照は、基本証券への参照または見積証券への参照の少なくとも一方を含み、
ｂ．前記第一のコンピュータプロセッサは、更に、前記有効期限タイムスタンプ以降に前記支払額を計算する、
装置。
【請求項２４】
転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を円滑化する装置であって、前記転送メカニズムが、前記装置、前記第一のクライアント、および第二のクライアントによってそれぞれコンピュータネットワークを介してアクセス可能な分散型デジタル通貨を含む、装置であって、
ａ．取引記録セクタと第一の非対称キーペアを記憶する第一のキーペアセクタとを有する第一のメモリであって、前記第一の非対称キーペアは、第一のプライベートキーおよび第一のパブリックキーを有する、第一のメモリと、
ｂ．支払額を決定するための条件を受け取る第一のネットワークインターフェースであって、前記条件は、
ｉ．第一の元本額および第二の元本額の少なくとも一方と、
ｉｉ．第一のデータソースおよび第二のデータソースの少なくとも一方への参照と、前記第一のデータソースは、第一の証券に関するデータを記憶する第一のデータベースを有し、前記第二のデータソースは、第二の証券に関するデータを記憶する第二のデータベースを有する、
ｉｉｉ．有効期限タイムスタンプと、を含む、第一のネットワークインターフェースと、
ｃ．前記第一のメモリおよび前記第一のネットワークインターフェースに結合された第一のコンピュータプロセッサであって、
ｉ．支払機能を、
Ａ．前記第一の元本額および前記第二の元本額の少なくとも一方、および
Ｂ．前記第一のデータソースおよび前記第二のデータソースの少なくとも一方からの値、に適用することにより、一つ以上の支払額を計算し、
ｉｉ．前記第一のキーペアセクタから前記第一のプライベートキーを読み取り、
ｉｉｉ．前記第一のプライベートキーから第一の暗号署名を計算し、
ｉｖ．未完了の支払取引記録を作成し、前記未完了の支払取引記録は、
Ａ．約定取引から受け取る約定額、
Ｂ．前記一つ以上の支払額、および
Ｃ．前記第一の暗号署名、を含む、
ｖ．前記未完了の支払取引記録を前記第一のクライアントまたは前記第二のクライアントの少なくとも一方に発行する、第一のコンピュータプロセッサと、
を有する、
ここで、前記第一のクライアントは、
ａ．第二の非対称キーペアを記憶する第二のキーペアセクタを有する第二のメモリであ

って、前記第二の非対称キーペアは、第二のプライベートキーおよび第二のパブリックキーを有する、第二のメモリと、
ｂ．第二のネットワークインターフェースと、
ｃ．前記第二のメモリおよび前記第二のネットワークインターフェースに結合された第二のコンピュータプロセッサであって、
ｉ．前記第二のキーペアセクタから前記第二のプライベートキーを読み取り、
ｉｉ．前記未完了の支払取引記録を読み取り、
ｉｉｉ．前記第二のプライベートキーから第二の暗号署名を計算し、
ｉｖ．完了した支払取引記録を作成し、前記完了した支払取引記録は、
Ａ．前記約定額、
Ｂ．前記一つ以上の支払額、
Ｃ．前記第一の暗号署名、および
Ｄ．前記第二の暗号署名、を含む、
ｖ．前記完了した支払取引記録を前記転送メカニズムに提出することにより支払取引を作成する、第二のコンピュータプロセッサと、を有し、
前記第二のクライアントは、
ａ．第三の非対称キーペアを記憶する第三のキーペアセクタを有する第三のメモリであって、前記第三の非対称キーペアは、第三のプライベートキーおよび第三のパブリックキーを有する、第三のメモリと、
ｂ．第三のネットワークインターフェースと、
ｃ．前記第三のメモリおよび前記第三のネットワークインターフェースに結合された第三のコンピュータプロセッサであって、前記第三のキーペアセクタから前記第三のプライベートキーを読み取る、第三のコンピュータプロセッサと、を有し、
前記装置、前記第一のクライアント、および前記第二のクライアントは、前記第一のネットワークインターフェース、前記第二のネットワークインターフェース、および前記第三のネットワークインターフェースをそれぞれ介して前記コンピュータネットワークに結合されており、
前記第一のコンピュータプロセッサは、前記支払機能を
ｉ．前記第一の元本額、および
ｉｉ．前記第一の証券の前記値
に適用することにより、前記一つ以上の支払額を計算し、
ａ．前記第一のキーペアセクタは、更に、第四の非対称キーペアを記憶し、前記第四の非対称キーペアは、第四のプライベートキーおよび第四のパブリックキーを有する、
ｂ．前記第一のコンピュータプロセッサは、更に、
ｉ．前記第一のキーペアセクタから前記第四のプライベートキーを読み取り、
ｉｉ．前記第四のプライベートキーから第三の暗号署名を計算し、
ｉｉｉ．約定取引記録を作成し、前記約定取引記録は、
Ａ．前記第一の元本額、
Ｂ．前記約定額、および
Ｃ．前記第三の暗号署名、を含む、
ｉｖ．前記約定取引記録を前記転送メカニズムに提出することにより前記約定取引を作成し、
前記第一の非対称キーペアは、前記第四の非対称キーペアと同一であり、前記第一のプライベートキーは、前記第四のプライベートキーと同一であり、前記第一のパブリックキーは、前記第四のパブリックキーと同一であり、
ａ．前記第一のデータソースまたは前記第二のデータソースへの前記参照は、基本証券への参照または見積証券への参照の少なくとも一方を含み、
ｂ．前記第一のコンピュータプロセッサは、更に、前記有効期限タイムスタンプ以降に前記支払額を計算する、
装置。

【請求項２５】
転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を円滑化する装置であって、前記転送メカニズムが、前記装置、前記第一のクライアント、および第二のクライアントによってそれぞれコンピュータネットワークを介してアクセス可能な分散型デジタル通貨を含む、装置であって、
ａ．取引記録セクタと第一の非対称キーペアを記憶する第一のキーペアセクタとを有する第一のメモリであって、前記第一の非対称キーペアは、第一のプライベートキーおよび第一のパブリックキーを有する、第一のメモリと、
ｂ．支払額を決定するための条件を受け取る第一のネットワークインターフェースであって、前記条件は、
ｉ．第一の元本額および第二の元本額の少なくとも一方と、
ｉｉ．第一のデータソースおよび第二のデータソースの少なくとも一方への参照と、前記第一のデータソースは、第一の証券に関するデータを記憶する第一のデータベースを有し、前記第二のデータソースは、第二の証券に関するデータを記憶する第二のデータベースを有する、
ｉｉｉ．有効期限タイムスタンプと、を含む、第一のネットワークインターフェースと、
ｃ．前記第一のメモリおよび前記第一のネットワークインターフェースに結合された第一のコンピュータプロセッサであって、
ｉ．支払機能を、
Ａ．前記第一の元本額および前記第二の元本額の少なくとも一方、および
Ｂ．前記第一のデータソースおよび前記第二のデータソースの少なくとも一方からの値、に適用することにより、一つ以上の支払額を計算し、
ｉｉ．前記第一のキーペアセクタから前記第一のプライベートキーを読み取り、
ｉｉｉ．前記第一のプライベートキーから第一の暗号署名を計算し、
ｉｖ．未完了の支払取引記録を作成し、前記未完了の支払取引記録は、
Ａ．約定取引から受け取る約定額、
Ｂ．前記一つ以上の支払額、および
Ｃ．前記第一の暗号署名、を含む、
ｖ．前記未完了の支払取引記録を前記第一のクライアントまたは前記第二のクライアントの少なくとも一方に発行する、第一のコンピュータプロセッサと、
を有する、
ここで、前記第一のクライアントは、
ａ．第二の非対称キーペアを記憶する第二のキーペアセクタを有する第二のメモリであって、前記第二の非対称キーペアは、第二のプライベートキーおよび第二のパブリックキーを有する、第二のメモリと、
ｂ．第二のネットワークインターフェースと、
ｃ．前記第二のメモリおよび前記第二のネットワークインターフェースに結合された第二のコンピュータプロセッサであって、
ｉ．前記第二のキーペアセクタから前記第二のプライベートキーを読み取り、
ｉｉ．前記未完了の支払取引記録を読み取り、
ｉｉｉ．前記第二のプライベートキーから第二の暗号署名を計算し、
ｉｖ．完了した支払取引記録を作成し、前記完了した支払取引記録は、
Ａ．前記約定額、
Ｂ．前記一つ以上の支払額、
Ｃ．前記第一の暗号署名、および
Ｄ．前記第二の暗号署名、を含む、
ｖ．前記完了した支払取引記録を前記転送メカニズムに提出することにより支払取引を作成する、第二のコンピュータプロセッサと、を有し、

前記第二のクライアントは、
ａ．第三の非対称キーペアを記憶する第三のキーペアセクタを有する第三のメモリであって、前記第三の非対称キーペアは、第三のプライベートキーおよび第三のパブリックキーを有する、第三のメモリと、
ｂ．第三のネットワークインターフェースと、
ｃ．前記第三のメモリおよび前記第三のネットワークインターフェースに結合された第三のコンピュータプロセッサであって、前記第三のキーペアセクタから前記第三のプライベートキーを読み取る、第三のコンピュータプロセッサと、を有し、
前記装置、前記第一のクライアント、および前記第二のクライアントは、前記第一のネットワークインターフェース、前記第二のネットワークインターフェース、および前記第三のネットワークインターフェースをそれぞれ介して前記コンピュータネットワークに結合されており、
前記第一のコンピュータプロセッサは、前記支払機能を
ｉ．前記第一の元本額、および
ｉｉ．前記第一の証券の前記値
に適用することにより、前記一つ以上の支払額を計算し、
前記第一のコンピュータプロセッサは、更に、
ａ．前記第一のプライベートキーから第三の暗号署名を計算し、
ｂ．未完了の払戻取引記録を作成し、前記未完了の払戻取引記録は、
ｉ．前記約定取引から受け取る前記約定額、
ｉｉ．払戻額、
ｉｉｉ．前記第三の暗号署名、および
ｉｖ．ロックタイム、を含む、
ｃ．前記未完了の払戻取引記録を前記第一のクライアントまたは前記第二のクライアントの少なくとも一方に発行する、
装置。
【請求項２６】
ａ．前記第一のキーペアセクタは、更に、第四の非対称キーペアを記憶し、前記第四の非対称キーペアは、第四のプライベートキーおよび第四のパブリックキーを有する、
ｂ．前記第一のコンピュータプロセッサは、更に、
ｉ．前記第一のキーペアセクタから前記第四のプライベートキーを読み取り、
ｉｉ．前記第四のプライベートキーから第四の暗号署名を計算し、
ｉｉｉ．約定取引記録を作成し、前記約定取引記録は、
Ａ．前記第一の元本額、
Ｂ．前記約定額、および
Ｃ．前記第四の暗号署名、を含む、
ｉｖ．前記約定取引記録を前記転送メカニズムに提出することにより前記約定取引を作成する、
請求項２５に記載の装置。
【請求項２７】
前記第一の非対称キーペアは、前記第四の非対称キーペアと同一であり、前記第一のプライベートキーは、前記第四のプライベートキーと同一であり、前記第一のパブリックキーは、前記第四のパブリックキーと同一である、
請求項２６に記載の装置。
【請求項２８】
ａ．前記第一のデータソースまたは前記第二のデータソースへの前記参照は、基本証券への参照および見積証券への参照の少なくとも一方を含み、
ｂ．前記第一のコンピュータプロセッサは、更に、前記有効期限タイムスタンプ以降に前記支払額を計算する、
請求項２６に記載の装置。

【請求項２９】
ａ．前記第一のキーペアセクタは、更に、第四の非対称キーペアを記憶し、前記第四の非対称キーペアは、第四のプライベートキーおよび第四のパブリックキーを有する、
ｂ．前記第一のコンピュータプロセッサは、更に、
ｉ．前記第一のキーペアセクタから前記第四のプライベートキーを読み取り、
ｉｉ．前記第四のプライベートキーから第四の暗号署名を計算し、
ｉｉｉ．約定取引記録を作成し、前記約定取引記録は、
Ａ．前記第一の元本額、
Ｂ．前記約定額、および
Ｃ．前記第四の暗号署名、を含む、
ｉｖ．前記約定取引記録を前記転送メカニズムに提出することにより前記約定取引を作成し、
前記第一の非対称キーペアは、前記第四の非対称キーペアと同一であり、前記第一のプライベートキーは、前記第四のプライベートキーと同一であり、前記第一のパブリックキーは、前記第四のパブリックキーと同一であり、
ａ．前記第一のデータソースまたは前記第二のデータソースへの前記参照は、基本証券への参照および見積証券への参照の少なくとも一方を含み、
ｂ．前記第一のコンピュータプロセッサは、更に、前記有効期限タイムスタンプ以降に前記支払額を計算する、
請求項２５に記載の装置。
【請求項３０】
転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を円滑化するシステムであって、前記転送メカニズムは、ファシリテータ、前記第一のクライアント、および第二のクライアントによってそれぞれコンピュータネットワークを介してアクセス可能な分散型デジタル通貨を含み、前記システムは、前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントを有し、
ａ．前記ファシリテータは、
ｉ．取引記録セクタと第一の非対称キーペアを記憶する第一のキーペアセクタとを有する第一のメモリであって、前記第一の非対称キーペアは、第一のプライベートキーおよび第一のパブリックキーを有する、第一のメモリと、
ｉｉ．支払額を決定するための条件を受け取る第一のネットワークインターフェースであって、前記条件は、
Ａ．第一の元本額および第二の元本額の少なくとも一方と、
Ｂ．第一のデータソースおよび第二のデータソースの少なくとも一方への参照と、前記第一のデータソースは、第一の証券に関するデータを記憶する第一のデータベースを有し、前記第二のデータソースは、第二の証券に関するデータを記憶する第二のデータベースを有する、
Ｃ．有効期限タイムスタンプと、を含む、第一のネットワークインターフェースと、
ｉｉｉ．前記第一のメモリおよび前記第一のネットワークインターフェースに結合された第一のコンピュータプロセッサであって、
Ａ．支払機能を、
前記第一の元本額および前記第二の元本額の少なくとも一方、および
前記第一のデータソースおよび前記第二のデータソースの少なくとも一方からの値
に適用することにより、一つ以上の支払額を計算し、
Ｂ．前記第一のキーペアセクタから前記第一のプライベートキーを読み取り、
Ｃ．前記第一のプライベートキーから第一の暗号署名を計算し、
Ｄ．未完了の支払取引記録を作成し、前記未完了の支払取引記録は、

Ｉ．約定取引から受け取る約定額
ＩＩ．前記一つ以上の支払額、および
ＩＩＩ．前記第一の暗号署名、を含む、
Ｅ．前記未完了の支払取引記録を前記第一のクライアントまたは前記第二のクライアントの少なくとも一方に発行する、第一のコンピュータプロセッサと、
を有し、
ｂ．前記第一のクライアントは、
ｉ．第二の非対称キーペアを記憶する第二のキーペアセクタを有する第二のメモリであって、前記第二の非対称キーペアは、第二のプライベートキーおよび第二のパブリックキーを有する、第二のメモリと、
ｉｉ．第二のネットワークインターフェースと、
ｉｉｉ．前記第二のメモリおよび前記第二のネットワークインターフェースに結合された第二のコンピュータプロセッサであって、
Ａ．前記第二のキーペアセクタから前記第二のプライベートキーを読み取り、
Ｂ．前記未完了の支払取引記録を読み取り、
Ｃ．前記第二のプライベートキーから第二の暗号署名を計算し、
Ｄ．完了した支払取引記録を作成し、前記完了した支払取引記録は、
Ｉ．前記約定額、
ＩＩ．前記一つ以上の支払額、
ＩＩＩ．前記第一の暗号署名、および
ＩＶ．前記第二の暗号署名、を含む、
Ｅ．前記完了した支払取引記録を前記転送メカニズムに提出することにより支払取引を作成する、第二のコンピュータプロセッサと、
を有し、
ｃ．前記第二のクライアントは、
ｉ．第三の非対称キーペアを記憶する第三のキーペアセクタを有する第三のメモリであって、前記第三の非対称キーペアは、第三のプライベートキーおよび第三のパブリックキーを有する、第三のメモリと、
ｉｉ．第三のネットワークインターフェースと、
ｉｉｉ．前記第三のメモリおよび前記第三のネットワークインターフェースに結合された第三のコンピュータプロセッサであって、前記第三のキーペアセクタから前記第三のプライベートキーを読み取る、第三のコンピュータプロセッサと、を有し、
前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントは、前記第一のネットワークインターフェース、前記第二のネットワークインターフェース、および前記第三のネットワークインターフェースをそれぞれ介して前記コンピュータネットワークに結合されており、
前記第一のコンピュータプロセッサは、更に、
ａ．前記第一のプライベートキーから第三の暗号署名を計算し、
ｂ．未完了の払戻取引記録を作成し、前記未完了の払戻取引記録は、
ｉ．前記約定取引から受け取る前記約定額、
ｉｉ．払戻額、および
ｉｉｉ．前記第三の暗号署名、を含む、
ｃ．前記未完了の払戻取引記録を前記第一のクライアントまたは前記第二のクライアントの少なくとも一方に発行し、
ａ．前記第一のキーペアセクタは、更に、第四の非対称キーペアを記憶し、前記第四の非対称キーペアは、第四のプライベートキーおよび第四のパブリックキーを有する、
ｂ．前記第一のコンピュータプロセッサは、更に、
ｉ．前記支払機能を
Ａ．前記第一の元本額、および
Ｂ．前記第一の証券の前記値、

に適用することにより、前記一つ以上の支払額を計算し、
ｉｉ．前記第一のキーペアセクタから前記第四のプライベートキーを読み取り、
ｉｉｉ．前記第四のプライベートキーから第四の暗号署名を計算し、
ｉｖ．約定取引記録を作成し、前記約定取引記録は、
Ａ．前記第一の元本額、
Ｂ．前記約定額、および
Ｃ．前記第四の暗号署名、を含む、
ｖ．前記約定取引記録を前記転送メカニズムに提出することにより前記約定取引を作成し、
前記第二のコンピュータプロセッサは、
ａ．前記第二のプライベートキーから第五の暗号署名を計算し、
ｂ．第一の元本取引記録を作成し、前記第一の元本取引記録は、
ｉ．前記第一の元本額、および
ｉｉ．前記第五の暗号署名、を含む、
ｃ．前記第一の元本取引記録を前記転送メカニズムに提出することにより第一の元本取引を作成する、
システム。
【請求項３１】
ａ．前記第一のデータソースまたは前記第二のデータソースへの前記参照は、基本証券への参照および見積証券への参照の少なくとも一方を含み、
ｂ．前記第一のコンピュータプロセッサは、更に、前記有効期限タイムスタンプ以降に前記支払額を計算する、
請求項３０に記載のシステム。
【請求項３２】
前記第三のコンピュータプロセッサは、更に、
ｉ．前記第三のプライベートキーから第六の暗号署名を計算し、
ｉｉ．第二の元本取引記録を作成し、前記第二の元本取引記録は、
Ａ．前記第二の元本額、および
Ｂ．前記第六の暗号署名、を含む、
ｉｉｉ．前記第二の元本取引記録を前記転送メカニズムに提出することにより第二の元本取引を作成し、
請求項３０に記載のシステム。
【請求項３３】
ａ．前記第一のデータソースまたは前記第二のデータソースへの前記参照は、基本証券への参照および見積証券への参照の少なくとも一方を含み、
ｂ．前記第一のコンピュータプロセッサは、更に、前記有効期限タイムスタンプ以降に前記支払額を計算し、
ｃ．前記第三のコンピュータプロセッサは、更に、
ｉ．前記第三のプライベートキーから第六の暗号署名を計算し、
ｉｉ．第二の元本取引記録を作成し、前記第二の元本取引記録は、
Ａ．前記第二の元本額、および
Ｂ．前記第六の暗号署名、を含む、
ｉｉｉ．前記第二の元本取引記録を前記転送メカニズムに提出することにより第二の元本取引を作成し、
請求項３０に記載のシステム。
【請求項３４】
転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を円滑化するシステムであって、前記転送メカニズムは、ファシリテータ、前記第一のクライアント、および第二のクライアントによってそれぞれコンピュータネットワークを介してアクセス可能な分散型デジタル通貨

を含み、前記システムは、前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントを有し、
ａ．前記ファシリテータは、
ｉ．取引記録セクタと第一の非対称キーペアを記憶する第一のキーペアセクタとを有する第一のメモリであって、前記第一の非対称キーペアは、第一のプライベートキーおよび第一のパブリックキーを有する、第一のメモリと、
ｉｉ．支払額を決定するための条件を受け取る第一のネットワークインターフェースであって、前記条件は、
Ａ．第一の元本額および第二の元本額の少なくとも一方と、
Ｂ．第一のデータソースおよび第二のデータソースの少なくとも一方への参照と、前記第一のデータソースは、第一の証券に関するデータを記憶する第一のデータベースを有し、前記第二のデータソースは、第二の証券に関するデータを記憶する第二のデータベースを有する、
Ｃ．有効期限タイムスタンプと、を含む、第一のネットワークインターフェースと、
ｉｉｉ．前記第一のメモリおよび前記第一のネットワークインターフェースに結合された第一のコンピュータプロセッサであって、
Ａ．支払機能を、
前記第一の元本額および前記第二の元本額の少なくとも一方、および
前記第一のデータソースおよび前記第二のデータソースの少なくとも一方からの値
に適用することにより、一つ以上の支払額を計算し、
Ｂ．前記第一のキーペアセクタから前記第一のプライベートキーを読み取り、
Ｃ．前記第一のプライベートキーから第一の暗号署名を計算し、
Ｄ．未完了の支払取引記録を作成し、前記未完了の支払取引記録は、
Ｉ．約定取引から受け取る約定額
ＩＩ．前記一つ以上の支払額、および
ＩＩＩ．前記第一の暗号署名、を含む、
Ｅ．前記未完了の支払取引記録を前記第一のクライアントまたは前記第二のクライアントの少なくとも一方に発行する、第一のコンピュータプロセッサと、
を有し、
ｂ．前記第一のクライアントは、
ｉ．第二の非対称キーペアを記憶する第二のキーペアセクタを有する第二のメモリであって、前記第二の非対称キーペアは、第二のプライベートキーおよび第二のパブリックキーを有する、第二のメモリと、
ｉｉ．第二のネットワークインターフェースと、
ｉｉｉ．前記第二のメモリおよび前記第二のネットワークインターフェースに結合された第二のコンピュータプロセッサであって、
Ａ．前記第二のキーペアセクタから前記第二のプライベートキーを読み取り、
Ｂ．前記未完了の支払取引記録を読み取り、
Ｃ．前記第二のプライベートキーから第二の暗号署名を計算し、
Ｄ．完了した支払取引記録を作成し、前記完了した支払取引記録は、
Ｉ．前記約定額、
ＩＩ．前記一つ以上の支払額、
ＩＩＩ．前記第一の暗号署名、および
ＩＶ．前記第二の暗号署名、を含む、
Ｅ．前記完了した支払取引記録を前記転送メカニズムに提出することにより支払取引を作成する、第二のコンピュータプロセッサと、
を有し、
ｃ．前記第二のクライアントは、

ｉ．第三の非対称キーペアを記憶する第三のキーペアセクタを有する第三のメモリであって、前記第三の非対称キーペアは、第三のプライベートキーおよび第三のパブリックキーを有する、第三のメモリと、
ｉｉ．第三のネットワークインターフェースと、
ｉｉｉ．前記第三のメモリおよび前記第三のネットワークインターフェースに結合された第三のコンピュータプロセッサであって、前記第三のキーペアセクタから前記第三のプライベートキーを読み取る、第三のコンピュータプロセッサと、を有し、
前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントは、前記第一のネットワークインターフェース、前記第二のネットワークインターフェース、および前記第三のネットワークインターフェースをそれぞれ介して前記コンピュータネットワークに結合されており、
前記ファシリテータと前記第一のクライアントは、同一の装置であり、
前記第一のコンピュータプロセッサと前記第二のコンピュータプロセッサは、同一のプロセッサであり、
前記第一のメモリと前記第二のメモリは、同一のメモリであり、
前記第一のネットワークインターフェースと前記第二のネットワークインターフェースは、同一のネットワークインターフェースであり、
前記第一のコンピュータプロセッサは、更に、
ａ．前記第一のプライベートキーから第三の暗号署名を計算し、
ｂ．未完了の払戻取引記録を作成し、前記未完了の払戻取引記録は、
ｉ．前記約定取引から受け取る前記約定額、
ｉｉ．払戻額、および
ｉｉｉ．前記第三の暗号署名、を含む、
ｃ．前記未完了の払戻取引記録を前記第一のクライアントおよび前記第二のクライアントの少なくとも一方に発行する、
システム。
【請求項３５】
ａ．前記第一のデータソースまたは前記第二のデータソースへの前記参照は、基本証券への参照および見積証券への参照の少なくとも一方を含み、
ｂ．前記第一のコンピュータプロセッサは、更に、前記有効期限タイムスタンプ以降に前記支払額を計算し、
ｃ．前記第二のコンピュータプロセッサは、更に、
ｉ．前記第二のプライベートキーから第四の暗号署名を計算し、
ｉｉ．第一の元本取引記録を作成し、前記第一の元本取引記録は、
Ａ．前記第一の元本額、および
Ｂ．前記第四の暗号署名、を含む、
ｉｉｉ．前記第一の元本取引記録を前記転送メカニズムに提出することにより第一の元本取引を作成し、
ｄ．前記第三のコンピュータプロセッサは、更に、
ｉ．前記第三のプライベートキーから第五の暗号署名を計算し、
ｉｉ．第二の元本取引記録を作成し、前記第二の元本取引記録は、
Ａ．前記第二の元本額、および
Ｂ．前記第五の暗号署名、を含む、
ｉｉｉ．前記第二の元本取引記録を前記転送メカニズムに提出することにより第二の元本取引を作成する、
請求項３４に記載のシステム。
【請求項３６】
転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を円滑化するシステムであって、前記転送メカニズムは、ファシリテータ、前記第一のクライアント、および第二のクライアント

によってそれぞれコンピュータネットワークを介してアクセス可能な分散型デジタル通貨を含み、前記システムは、前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントを有し、

ａ．前記ファシリテータは、

ｉ．取引記録セクタと第一の非対称キーペアを記憶する第一のキーペアセクタとを有する第一のメモリであって、前記第一の非対称キーペアは、第一のプライベートキーおよび第一のパブリックキーを有する、第一のメモリと、

ｉｉ．支払額を決定するための条件を受け取る第一のネットワークインターフェースであって、前記条件は、

Ａ．第一の元本額および第二の元本額の少なくとも一方と、

Ｂ．第一のデータソースおよび第二のデータソースの少なくとも一方への参照と、前記第一のデータソースは、第一の証券に関するデータを記憶する第一のデータベースを有し、前記第二のデータソースは、第二の証券に関するデータを記憶する第二のデータベースを有する、

Ｃ．有効期限タイムスタンプと、を含む、第一のネットワークインターフェースと、

ｉｉｉ．前記第一のメモリおよび前記第一のネットワークインターフェースに結合された第一のコンピュータプロセッサであって、

Ａ．支払機能を、

前記第一の元本額および前記第二の元本額の少なくとも一方、および

前記第一のデータソースおよび前記第二のデータソースの少なくとも一方からの値

に適用することにより、一つ以上の支払額を計算し、

Ｂ．前記第一のキーペアセクタから前記第一のプライベートキーを読み取り、

Ｃ．前記第一のプライベートキーから第一の暗号署名を計算し、

Ｄ．未完了の支払取引記録を作成し、前記未完了の支払取引記録は、

Ｉ．約定取引から受け取る約定額

ＩＩ．前記一つ以上の支払額、および

ＩＩＩ．前記第一の暗号署名、を含む、

Ｅ．前記未完了の支払取引記録を前記第一のクライアントまたは前記第二のクライアントの少なくとも一方に発行する、第一のコンピュータプロセッサと、

を有し、

ｂ．前記第一のクライアントは、

ｉ．第二の非対称キーペアを記憶する第二のキーペアセクタを有する第二のメモリであって、前記第二の非対称キーペアは、第二のプライベートキーおよび第二のパブリックキーを有する、第二のメモリと、

ｉｉ．第二のネットワークインターフェースと、

ｉｉｉ．前記第二のメモリおよび前記第二のネットワークインターフェースに結合された第二のコンピュータプロセッサであって、

Ａ．前記第二のキーペアセクタから前記第二のプライベートキーを読み取り、

Ｂ．前記未完了の支払取引記録を読み取り、

Ｃ．前記第二のプライベートキーから第二の暗号署名を計算し、

Ｄ．完了した支払取引記録を作成し、前記完了した支払取引記録は、

Ｉ．前記約定額、

ＩＩ．前記一つ以上の支払額、

ＩＩＩ．前記第一の暗号署名、および

ＩＶ．前記第二の暗号署名、を含む、

Ｅ．前記完了した支払取引記録を前記転送メカニズムに提出することにより支払取引を作成する、第二のコンピュータプロセッサと、

を有し、

ｃ．前記第二のクライアントは、
ｉ．第三の非対称キーペアを記憶する第三のキーペアセクタを有する第三のメモリであって、前記第三の非対称キーペアは、第三のプライベートキーおよび第三のパブリックキーを有する、第三のメモリと、
ｉｉ．第三のネットワークインターフェースと、
ｉｉｉ．前記第三のメモリおよび前記第三のネットワークインターフェースに結合された第三のコンピュータプロセッサであって、前記第三のキーペアセクタから前記第三のプライベートキーを読み取る、第三のコンピュータプロセッサと、を有し、
前記ファシリテータ、前記第一のクライアント、および前記第二のクライアントは、前記第一のネットワークインターフェース、前記第二のネットワークインターフェース、および前記第三のネットワークインターフェースをそれぞれ介して前記コンピュータネットワークに結合されており、
前記ファシリテータと前記第一のクライアントは、同一の装置であり、
前記第一のコンピュータプロセッサと前記第二のコンピュータプロセッサは、同一のプロセッサであり、
前記第一のメモリと前記第二のメモリは、同一のメモリであり、
前記第一のネットワークインターフェースと前記第二のネットワークインターフェースは、同一のネットワークインターフェースである、
ａ．前記第一のキーペアセクタは、更に、第四の非対称キーペアを記憶し、前記第四の非対称キーペアは、第四のプライベートキーおよび第四のパブリックキーを有する、
ｂ．前記第一のコンピュータプロセッサは、更に、
ｉ．前記支払機能を
Ａ．前記第一の元本額、および
Ｂ．前記第一の証券の前記値、
に適用することにより、前記一つ以上の支払額を計算し、
ｉｉ．前記第一のキーペアセクタから前記第四のプライベートキーを読み取り、
ｉｉｉ．前記第四のプライベートキーから第三の暗号署名を計算し、
ｉｖ．約定取引記録を作成し、前記約定取引記録は、
Ａ．前記第一の元本額、
Ｂ．前記約定額、および
Ｃ．前記第三の暗号署名、を含む、
ｖ．前記約定取引記録を前記転送メカニズムに提出することにより前記約定取引を作成し、
前記第二のコンピュータプロセッサは、
ａ．前記第二のプライベートキーから第四の暗号署名を計算し、
ｂ．第一の元本取引記録を作成し、前記第一の元本取引記録は、
ｉ．前記第一の元本額、および
ｉｉ．前記第四の暗号署名、を含む、
ｃ．前記第一の元本取引記録を前記転送メカニズムに提出することにより第一の元本取引を作成し、
ａ．前記第一のデータソースまたは前記第二のデータソースへの前記参照は、基本証券への参照および見積証券への参照の少なくとも一方を含み、
ｂ．前記第一のコンピュータプロセッサは、更に、前記有効期限タイムスタンプ以降に前記支払額を計算し、
ａ．前記第三のコンピュータプロセッサは、更に、
ｉ．前記第三のプライベートキーから第五の暗号署名を計算し、
ｉｉ．第二の元本取引記録を作成し、前記第二の元本取引記録は、
Ａ．前記第二の元本額、および
Ｂ．前記第五の暗号署名、を含む、
ｉｉｉ．前記第二の元本取引記録を前記転送メカニズムに提出することにより第二の

元本取引を作成する、
システム。
【請求項３７】
転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を、円滑化するシステムによって実行される方法であって、前記転送メカニズムが、ファシリテータ、前記第一のクライアント、および第二のクライアントによってそれぞれコンピュータネットワークを介してアクセス可能な分散型デジタル通貨を含む、方法であって、
前記第一のクライアントが、第一の非対称キーペアを第一のメモリの第一のキーペアセクタに記憶するステップであって、前記第一の非対称キーペアは、第一のパブリックキーおよび第一のプライベートキーを有する、ステップと、
前記ファシリテータが、第二の非対称キーペアを第二のメモリの第二のキーペアセクタに記憶するステップであって、前記第二の非対称キーペアは、第二のパブリックキーおよび第二のプライベートキーを有する、ステップと、
前記ファシリテータが、第三の非対称キーペアを前記第二のキーペアセクタに記憶するステップであって、前記第三の非対称キーペアは、第三のパブリックキーおよび第三のプライベートキーを有する、ステップと、
前記第一のクライアントが、第四の非対称キーペアを第三のメモリの第三のキーペアセクタに記憶するステップであって、前記第四の非対称キーペアは、第四のパブリックキーおよび第四のプライベートキーを有する、ステップと、
前記第一のクライアントが、ネットワークインターフェースを介して支払額を決定するための条件を送信するステップであって、前記条件は、
ｉ．第一の元本額および第二の元本額の少なくとも一方と、
ｉｉ．第一のデータソースおよび第二のデータソースの少なくとも一方への参照と、前記第一のデータソースは、証券に関するデータを記憶する第一のデータベースを有し、前記第二のデータソースは、第二の証券に関するデータを記憶する第二のデータベースを有する、
ｉｉｉ．有効期限タイムスタンプと、を含む、ステップと、
前記ファシリテータが、前記条件を第二のネットワークインターフェースを介して受け取るステップと、
前記ファシリテータが、支払機能を、
ｉ．前記第一の元本額および前記第二の元本額の少なくとも一方、および
ｉｉ．前記第一のデータソースおよび前記第二のデータソースの少なくとも一方からの値、に適用することにより、一つ以上の支払額を計算するステップと、
前記第一のクライアントが、前記第一のキーペアセクタから前記第一のプライベートキーを読み取るステップと、
前記ファシリテータが、前記第一のプライベートキーから第一の暗号署名を計算するステップと、
前記第一のクライアントが、第一の元本取引記録を作成するステップであって、前記第一の元本取引記録は、
ｉ．前記第一の元本額、および
ｉｉ．前記第一の暗号署名、を含む、ステップと、
前記第一のクライアントが、前記第一の元本取引記録を前記転送メカニズムに提出することにより第一の元本取引を作成するステップと、
前記ファシリテータが、前記第二のキーペアセクタから前記第二のプライベートキーを読み取るステップと、
前記ファシリテータが、前記第二のプライベートキーから第二の暗号署名を計算するステップと、
前記ファシリテータが、約定取引記録を作成するステップであって、前記約定取引記録は、

ｉ．前記第一の元本額、
ｉｉ．約定額、および
ｉｉｉ．前記第二の暗号署名、を含む、ステップと、
前記ファシリテータが、前記約定取引記録を前記転送メカニズムに提出することにより約定取引を作成するステップと、
前記ファシリテータが、前記第一のデータソースから前記証券の値を引き出すステップと、
前記ファシリテータが、前記第二のキーペアセクタから前記第三のプライベートキーを読み取るステップと、
前記ファシリテータが、前記第二のプライベートキーから第三の暗号署名を計算するステップと、
前記ファシリテータが、未完了の支払取引記録を作成するステップであって、前記未完了の支払取引記録は、
ｉ．前記約定取引から受け取る前記約定額、
ｉｉ．前記一つ以上の支払額、および
ｉｉｉ．前記第三の暗号署名、を含む、ステップと、
前記ファシリテータが、前記未完了の支払取引記録を前記第一のクライアントおよび前記第二のクライアントの少なくとも一方に発行するステップと、
前記第一のクライアントが、前記未完了の支払取引記録を読み取るステップと、
前記第一のクライアントが、前記第三のキーペアセクタから前記第四のプライベートキーを読み取るステップと、
前記第一のクライアントが、前記第四のプライベートキーから第四の暗号署名を計算するステップと、
前記第一のクライアントが、完了した支払取引記録を作成するステップであって、前記完了した支払取引記録は、
ｉ．前記約定額、
ｉｉ．前記一つ以上の支払額、
ｉｉｉ．前記第三の暗号署名、および
ｉｖ．前記第四の暗号署名、を含む、ステップと、
前記第一のクライアントが、前記完了した支払取引記録を前記転送メカニズムに提出することにより支払取引を作成するステップと、
前記ファシリテータが、前記第三のプライベートキーから第五の暗号署名を計算するステップと、
前記ファシリテータが、未完了の払戻取引記録を作成するステップであって、前記未完了の払戻取引記録は、
ｉ．前記約定取引から受け取る前記約定額、
ｉｉ．払戻額、
ｉｉｉ．前記第五の暗号署名、および
ｉｖ．ロックタイム、を含む、ステップと、
前記ファシリテータが、前記未完了の払戻取引記録を発行するステップと、
ａ．前記第二の非対称キーペアと前記第三の非対称キーペアは、同一のキーペアであり、前記第二のプライベートキーと前記第三のプライベートキーは、同一のキーであり、前記第二のパブリックキーと前記第三のパブリックキーは、同一のキーである、
ｂ．前記第一の非対称キーペアと前記第四の非対称キーペアは、同一のキーペアであり、前記第一のプライベートキーと前記第四のプライベートキーは、同一のキーであり、前記第一のパブリックキーと前記第四のパブリックキーは、同一のキーである、
ｃ．前記第一のメモリと前記第三のメモリは、同一のメモリであり、前記第一のキーペアセクタと前記第三のキーペアセクタは、同一のセクタである、
の少なくとも一つである、方法。

【請求項３８】

前記第二のクライアントが、第五の非対称キーペアを第四のメモリの第四のキーペアセクタに記憶するステップであって、前記第五の非対称キーペアは、第五のプライベートキーおよび第五のパブリックキーを有する、ステップと、
前記第二のクライアントが、前記第四のキーペアセクタから前記第五のプライベートキーを読み取るステップと、
前記第二のクライアントが、前記第五のプライベートキーから第五の暗号署名を計算するステップと、
前記第二のクライアントが、第二の元本取引記録を作成するステップであって、前記第二の元本取引記録は、
ｉ．前記第二の元本額、および
ｉｉ．前記第五の暗号署名、を含む、ステップと、
前記第二のクライアントが、前記第二の元本取引記録を前記転送メカニズムに提出することにより第二の元本取引を作成するステップと、
前記ファシリテータが、前記支払機能を、
ｉ．前記証券の前記値、ならびに
Ａ．前記第一の元本額、または
Ｂ．前記第二の元本額、の少なくとも一方
に適用することにより、一つ以上の支払額を計算するステップと、
を更に有する
請求項３７に記載の方法。

【請求項３９】
転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を、円滑化するシステムによって実行される方法であって、前記転送メカニズムが、ファシリテータ、前記第一のクライアント、および第二のクライアントによってそれぞれコンピュータネットワークを介してアクセス可能な分散型デジタル通貨を含む、方法であって、
前記第一のクライアントが、第一の非対称キーペアを第一のメモリの第一のキーペアセクタに記憶するステップであって、前記第一の非対称キーペアは、第一のパブリックキーおよび第一のプライベートキーを有する、ステップと、
前記ファシリテータが、第二の非対称キーペアを第二のメモリの第二のキーペアセクタに記憶するステップであって、前記第二の非対称キーペアは、第二のパブリックキーおよび第二のプライベートキーを有する、ステップと、
前記ファシリテータが、第三の非対称キーペアを前記第二のキーペアセクタに記憶するステップであって、前記第三の非対称キーペアは、第三のパブリックキーおよび第三のプライベートキーを有する、ステップと、
前記第一のクライアントが、第四の非対称キーペアを第三のメモリの第三のキーペアセクタに記憶するステップであって、前記第四の非対称キーペアは、第四のパブリックキーおよび第四のプライベートキーを有する、ステップと、
前記第一のクライアントが、ネットワークインターフェースを介して支払額を決定するための条件を送信するステップであって、前記条件は、
ｉ．第一の元本額および第二の元本額の少なくとも一方と、
ｉｉ．第一のデータソースおよび第二のデータソースの少なくとも一方への参照と、前記第一のデータソースは、証券に関するデータを記憶する第一のデータベースを有し、前記第二のデータソースは、第二の証券に関するデータを記憶する第二のデータベースを有する、
ｉｉｉ．有効期限タイムスタンプと、を含む、ステップと、
前記ファシリテータが、前記条件を第二のネットワークインターフェースを介して受け取るステップと、
前記ファシリテータが、支払機能を、
ｉ．前記第一の元本額および前記第二の元本額の少なくとも一方、および

ｉｉ．前記第一のデータソースおよび前記第二のデータソースの少なくとも一方からの値、に適用することにより、一つ以上の支払額を計算するステップと、
前記第一のクライアントが、前記第一のキーペアセクタから前記第一のプライベートキーを読み取るステップと、
前記ファシリテータが、前記第一のプライベートキーから第一の暗号署名を計算するステップと、
前記第一のクライアントが、第一の元本取引記録を作成するステップであって、前記第一の元本取引記録は、
ｉ．前記第一の元本額、および
ｉｉ．前記第一の暗号署名、を含む、ステップと、
前記第一のクライアントが、前記第一の元本取引記録を前記転送メカニズムに提出することにより第一の元本取引を作成するステップと、
前記ファシリテータが、前記第二のキーペアセクタから前記第二のプライベートキーを読み取るステップと、
前記ファシリテータが、前記第二のプライベートキーから第二の暗号署名を計算するステップと、
前記ファシリテータが、約定取引記録を作成するステップであって、前記約定取引記録は、
ｉ．前記第一の元本額、
ｉｉ．約定額、および
ｉｉｉ．前記第二の暗号署名、を含む、ステップと、
前記ファシリテータが、前記約定取引記録を前記転送メカニズムに提出することにより約定取引を作成するステップと、
前記ファシリテータが、前記第一のデータソースから前記証券の値を引き出すステップと、
前記ファシリテータが、前記第二のキーペアセクタから前記第三のプライベートキーを読み取るステップと、
前記ファシリテータが、前記第二のプライベートキーから第三の暗号署名を計算するステップと、
前記ファシリテータが、未完了の支払取引記録を作成するステップであって、前記未完了の支払取引記録は、
ｉ．前記約定取引から受け取る前記約定額、
ｉｉ．前記一つ以上の支払額、および
ｉｉｉ．前記第三の暗号署名、を含む、ステップと、
前記ファシリテータが、前記未完了の支払取引記録を前記第一のクライアントおよび前記第二のクライアントの少なくとも一方に発行するステップと、
前記第一のクライアントが、前記未完了の支払取引記録を読み取るステップと、
前記第一のクライアントが、前記第三のキーペアセクタから前記第四のプライベートキーを読み取るステップと、
前記第一のクライアントが、前記第四のプライベートキーから第四の暗号署名を計算するステップと、
前記第一のクライアントが、完了した支払取引記録を作成するステップであって、前記完了した支払取引記録は、
ｉ．前記約定額、
ｉｉ．前記一つ以上の支払額、
ｉｉｉ．前記第三の暗号署名、および
ｉｖ．前記第四の暗号署名、を含む、ステップと、
前記第一のクライアントが、前記完了した支払取引記録を前記転送メカニズムに提出することにより支払取引を作成するステップと、
前記第二のクライアントが、第五の非対称キーペアを第四のメモリの第四のキーペアセ

クタに記憶するステップであって、前記第五の非対称キーペアは、第五のプライベートキーおよび第五のパブリックキーを有する、ステップと、
前記第二のクライアントが、前記第四のキーペアセクタから前記第五のプライベートキーを読み取るステップと、
前記第二のクライアントが、前記第五のプライベートキーから第五の暗号署名を計算するステップと、
前記第二のクライアントが、第二の元本取引記録を作成するステップであって、前記第二の元本取引記録は、
ｉ．前記第二の元本額、および
ｉｉ．前記第五の暗号署名、を含む、ステップと、
前記第二のクライアントが、前記第二の元本取引記録を前記転送メカニズムに提出することにより第二の元本取引を作成するステップと、
前記ファシリテータが、前記支払機能を、
ｉ．前記証券の前記値、ならびに
Ａ．前記第一の元本額、または
Ｂ．前記第二の元本額、の少なくとも一方
に適用することにより、一つ以上の支払額を計算するステップと、
前記ファシリテータが、前記第三のプライベートキーから第六の暗号署名を計算するステップと、
前記ファシリテータが、未完了の払戻取引記録を作成するステップであって、前記未完了の払戻取引記録は、
ｉ．前記約定取引から受け取る前記約定額、
ｉｉ．一つ以上の払戻額、
ｉｉｉ．前記第六の暗号署名、および
ｉｖ．ロックタイム、を含む、ステップと、
前記ファシリテータが、前記未完了の払戻取引記録を発行するステップと、
を含み、
ａ．前記第二の非対称キーペアと前記第三の非対称キーペアは、同一の非対称キーペアであり、前記第二のプライベートキーと前記第三のプライベートキーは、同一のプライベートキーであり、前記第二のパブリックキーと前記第三のパブリックキーは、同一のパブリックキーである、
ｂ．前記第一の非対称キーペアと前記第四の非対称キーペアは、同一のキーペアであり、前記第一のプライベートキーと前記第四のプライベートキーは、同一のプライベートキーであり、前記第一のパブリックキーと前記第四のパブリックキーは、同一のパブリックキーである、
ｃ．前記第五の非対称キーペアと前記第四の非対称キーペアは、同一の非対称キーペアであり、前記第五のプライベートキーと前記第四のプライベートキーは、同一のプライベートキーであり、前記第五のパブリックキーと前記第四のパブリックキーは、同一のパブリックキーである、
ｄ．前記第一のメモリと前記第三のメモリは、同一のメモリであり、前記第一のキーペアセクタと前記第三のキーペアセクタは、同一のキーペアセクタである、
ｅ．前記第四のメモリと前記第三のメモリは、同一のメモリであり、前記第四のキーペアセクタと前記第三のキーペアセクタは、同一のキーペアセクタである、
の少なくとも一つである、
方法。
【請求項４０】
転送メカニズムによる、第一のクライアントを利用する第一の当事者と、第二のクライアントを利用する第二の当事者との間の価値転送を、円滑化するシステムによって実行される方法であって、前記転送メカニズムが、ファシリテータ、前記第一のクライアント、および第二のクライアントによってそれぞれコンピュータネットワークを介してアクセス

可能な分散型デジタル通貨を含む、方法であって、
前記第一のクライアントが、第一の非対称キーペアを第一のメモリの第一のキーペアセクタに記憶するステップであって、前記第一の非対称キーペアは、第一のパブリックキーおよび第一のプライベートキーを有する、ステップと、
前記ファシリテータが、第二の非対称キーペアを第二のメモリの第二のキーペアセクタに記憶するステップであって、前記第二の非対称キーペアは、第二のパブリックキーおよび第二のプライベートキーを有する、ステップと、
前記ファシリテータが、第三の非対称キーペアを前記第二のキーペアセクタに記憶するステップであって、前記第三の非対称キーペアは、第三のパブリックキーおよび第三のプライベートキーを有する、ステップと、
前記第一のクライアントが、第四の非対称キーペアを第三のメモリの第三のキーペアセクタに記憶するステップであって、前記第四の非対称キーペアは、第四のパブリックキーおよび第四のプライベートキーを有する、ステップと、
前記第一のクライアントが、ネットワークインターフェースを介して支払額を決定するための条件を送信するステップであって、前記条件は、
ｉ．第一の元本額および第二の元本額の少なくとも一方と、
ｉｉ．第一のデータソースおよび第二のデータソースの少なくとも一方への参照と、前記第一のデータソースは、証券に関するデータを記憶する第一のデータベースを有し、前記第二のデータソースは、第二の証券に関するデータを記憶する第二のデータベースを有する、
ｉｉｉ．有効期限タイムスタンプと、を含む、ステップと、
前記ファシリテータが、前記条件を第二のネットワークインターフェースを介して受け取るステップと、
前記ファシリテータが、支払機能を、
ｉ．前記第一の元本額および前記第二の元本額の少なくとも一方、および
ｉｉ．前記第一のデータソースおよび前記第二のデータソースの少なくとも一方からの値、に適用することにより、一つ以上の支払額を計算するステップと、
前記第一のクライアントが、前記第一のキーペアセクタから前記第一のプライベートキーを読み取るステップと、
前記ファシリテータが、前記第一のプライベートキーから第一の暗号署名を計算するステップと、
前記第一のクライアントが、第一の元本取引記録を作成するステップであって、前記第一の元本取引記録は、
ｉ．前記第一の元本額、および
ｉｉ．前記第一の暗号署名、を含む、ステップと、
ｋ．前記第一のクライアントが、前記第一の元本取引記録を前記転送メカニズムに提出することにより第一の元本取引を作成するステップと、
前記ファシリテータが、前記第二のキーペアセクタから前記第二のプライベートキーを読み取るステップと、
前記ファシリテータが、前記第二のプライベートキーから第二の暗号署名を計算するステップと、
前記ファシリテータが、約定取引記録を作成するステップであって、前記約定取引記録は、
ｉ．前記第一の元本額、
ｉｉ．約定額、および
ｉｉｉ．前記第二の暗号署名、を含む、ステップと、
前記ファシリテータが、前記約定取引記録を前記転送メカニズムに提出することにより約定取引を作成するステップと、
前記ファシリテータが、前記第一のデータソースから前記証券の値を引き出すステップと、

前記ファシリテータが、前記第二のキーペアセクタから前記第三のプライベートキーを読み取るステップと、
前記ファシリテータが、前記第二のプライベートキーから第三の暗号署名を計算するステップと、
前記ファシリテータが、未完了の支払取引記録を作成するステップであって、前記未完了の支払取引記録は、
ｉ．前記約定取引から受け取る前記約定額、
ｉｉ．前記一つ以上の支払額、および
ｉｉｉ．前記第三の暗号署名、を含む、ステップと、
前記ファシリテータが、前記未完了の支払取引記録を前記第一のクライアントおよび前記第二のクライアントの少なくとも一方に発行するステップと、
前記第一のクライアントが、前記未完了の支払取引記録を読み取るステップと、
前記第一のクライアントが、前記第三のキーペアセクタから前記第四のプライベートキーを読み取るステップと、
前記第一のクライアントが、前記第四のプライベートキーから第四の暗号署名を計算するステップと、
前記第一のクライアントが、完了した支払取引記録を作成するステップであって、前記完了した支払取引記録は、
ｉ．前記約定額、
ｉｉ．前記一つ以上の支払額、
ｉｉｉ．前記第三の暗号署名、および
ｉｖ．前記第四の暗号署名、を含む、ステップと、
前記第一のクライアントが、前記完了した支払取引記録を前記転送メカニズムに提出することにより支払取引を作成するステップと、
前記ファシリテータが、前記第三のプライベートキーから第五の暗号署名を計算するステップと、
前記ファシリテータが、未完了の払戻取引記録を作成するステップであって、前記未完了の払戻取引記録は、
ｉ．前記約定取引から受け取る前記約定額、
ｉｉ．払戻額、
ｉｉｉ．前記第五の暗号署名、および
ｉｖ．ロックタイム、を含む、ステップと、
前記ファシリテータが、前記未完了の払戻取引記録を発行するステップと、
前記第二のクライアントが、第五の非対称キーペアを第四のメモリの第四のキーペアセクタに記憶するステップであって、前記第五の非対称キーペアは、第五のプライベートキーおよび第五のパブリックキーを有する、ステップと、
前記第二のクライアントが、前記第四のキーペアセクタから前記第五のプライベートキーを読み取るステップと、
前記第二のクライアントが、前記第五のプライベートキーから第六の暗号署名を計算するステップと、
前記第二のクライアントが、第二の元本取引記録を作成するステップであって、前記第二の元本取引記録は、
ｉ．前記第二の元本額、および
ｉｉ．前記第六の暗号署名、を含む、ステップと、
前記第二のクライアントが、前記第二の元本取引記録を前記転送メカニズムに提出することにより第二の元本取引を作成するステップと、
前記ファシリテータが、前記支払機能を、
ｉ．前記証券の前記値、ならびに
Ａ．前記第一の元本額、または
Ｂ．前記第二の元本額、の少なくとも一方

に適用することにより、一つ以上の支払額を計算するステップと、
を含み、
ａ．前記第二の非対称キーペアと前記第三の非対称キーペアは、同一の非対称キーペアであり、前記第二のプライベートキーと前記第三のプライベートキーは、同一のプライベートキーであり、前記第二のパブリックキーと前記第三のパブリックキーは、同一のパブリックキーである、
ｂ．前記第一の非対称キーペアと前記第四の非対称キーペアは、同一のキーペアであり、前記第一のプライベートキーと前記第四のプライベートキーは、同一のプライベートキーであり、前記第一のパブリックキーと前記第四のパブリックキーは、同一のパブリックキーである、
ｃ．前記第五の非対称キーペアと前記第四の非対称キーペアは、同一の非対称キーペアであり、前記第五のプライベートキーと前記第四のプライベートキーは、同一のプライベートキーであり、前記第五のパブリックキーと前記第四のパブリックキーは、同一のパブリックキーである、
ｄ．前記第一のメモリと前記第三のメモリは、同一のメモリであり、前記第一のキーペアセクタと前記第三のキーペアセクタは、同一のキーペアセクタである、
ｅ．前記第四のメモリと前記第三のメモリは、同一のメモリであり、前記第四のキーペアセクタと前記第三のキーペアセクタは、同一のキーペアセクタである、
方法。

【発明の詳細な説明】

【技術分野】

【０００１】

関連する分野は、電気通信、デジタル通信、コンピュータ技術である。

【０００２】

優先権主張

本出願は２０１４年５月９日に出願された米国仮出願第６１／９９０，７９５号への優先権を主張する。この出願は、本明細書に完了に記載されているかのように、この段落で言及された全ての出願の開示内容が参照によって本願に組み込まれる。

【０００３】

著作権に関する声明

図を含むこの文書の全ての内容は米国および他国の法律に基づく著作権保護の対象であり、所有者は公的な政府記録に表示されているとおり、この文書の複製またはその開示に異論を唱えない。その他の権利はすべて著作者に帰属する。

【背景技術】

【０００４】

市場効率は上昇傾向にあり、それにより取引にかかるコストは当事者の相互信頼に比例して減少する傾向がある。しかし、市場規模の拡大に比例して金利は市場金利を上回る傾向にあり、したがって信頼度は低下する傾向にある。より大きな市場（非特許文献１）への効率的で生産的な参加にはこの信頼度の問題を緩和する必要があるが、それにはコストも伴う。

このコストは規模の経済によって減少することもよくあるが、今日でも取引相手、仲介業者、納品後の支払いにおける失敗、保証人の失敗、エスクローなどによるリスクに対する緩衝にはかなりの経費がかかる。

【０００５】

１９９０年代半ば以来、それまで互いを知らなかった当事者間によるインターネットを基本通信媒体として時には国境を越えて合意される取引による商業活動の爆発があった。当事者間の信頼を確立、維持することは重要な役割を果たし、伝統的で非効率な方法による様々な解決策が試みられた。

【０００６】

このような個人が影響し合う市場の中には金融商品（株式、債券、選択売買権、先物、

スワップ、アンカバー通過残高など）を取引するものがある。金融工学の出現により、個人や企業は取引への開始及び終了をプログラムされた条件やアルゴリズムによって自動化するなど、金融取引における演算を活用することができるようになった。しかしこの分野で技術の使用が爆発的に増加しても、そのような技術は従来の中央集中型市場の中に圧倒的に積み重なっている。殆どすべてが取引するためには比較的高いコストを課している。一部の規模が巨大な取引所などは「価値の高い」（すなわち、高額の）顧客が、あまり手練れでない、もしくは技術を持たない投資家より優先されることを売りにしているところもある。このような慣行の公平性に疑問を抱くものもいる。

【０００７】

さらに、国際貿易における契約強制にかかる費用は法外になりうるし、成功を予測するのも非常に難しいかもしれない。更に、売り手はある通貨を受け取ることを望んでいるのに、買い手は別の通貨を送ることを望んでいる可能性もある。他の通貨建ての通貨の価値は変動しやすいこともある。これまで遠隔地での取引で当事者がリスクを軽減する方法といえば、第三者の介入が多かった。そのような仕組みの一つは信用状（Ｌ／Ｃ）である。信用状は売り手が大きな注文をした買い手自体を必ずしも信用してはいないが、買い手が信用枠を設定した銀行は信用できる場合に有効である。買い手と銀行は、売り手が一定の条件を満たした際にその信用枠から資金を解放することに同意する。（多くの場合、特定の日時以前に銀行へ出荷の証拠を送ることが条件である）銀行は売り手に約束（信用状）を発行し、売り手と買い手は残りの条件に同意する。しかし、支払いは多くの場合合意よりも遅い日付に行われ、合意がなされた日付から支払いの間に為替が変動する可能性がある。このような為替レートの変動性に適切に対応する資源は最も規模の大きい機関しか持っていない。更に信用状と為替のために銀行が請求する金額も相当なものである。逆に仲介業者には、資金を解放する前に当該文書の真実性を独立して検証することができる自己利益のみに基づく文書審査官として効果的に働くための高い信頼性が求められ、このことによって、間違い、偽造または詐欺のリスクを売り手に多く残してしまう可能性がある。したがって信用状は相対的な通貨価値が大きく変動する可能性のある取引や消費者取引にはあまり適していない。

【０００８】

厳密に制御された資産の制作を約束し、厳密に定義された基準が満たされた場合に、第三者の介入を殆ど必要とせず、これまでのメカニズムに比べて非常に低い転送コストで資産の制御または所有権を移転する能力を持つ分散型のデジタル通貨（いわゆる仮想通貨）は比較的新しい生き物である。ビットコインとその派生（Ｅｔｈｅｒｅｕｍ，　Ｌｉｔｅｃｏｉｎなど）は最近急激に人気（と評価）が上昇したそのようなテクノロジーの一つだと言える。

【０００９】

それを非限定的な例として説明する目的で、これらの特定の分散型デジタル通貨は一般的に、ネットワークの参加者によって「検証」された全ての取引の「元帳」（「ブロックチェーン」と呼ばれる場合もある）の一部または全ての履歴を維持することによって機能している。本発明の範囲を超えたいくつかの例外を除き、取引はおおよそ以下のように機能する（非特許文献２）。取引は少なくとも一つの入力、出力によって構成され、入力は規則正しく適切に定義された実行可能な操作によってできる入力「スクリプト」によって構成される。出力はまたそのような操作が含まれる二つめの出力スクリプトによって構成される。新しい（子）取引は既存の（親）取引からの出力スクリプトと入力スクリプトを予測可能な方法で結合してできている。新しい取引はネットワークの参加者の大多数がそのコンビネーションが所定のルールに鑑みて受け入れることを合意した場合に有効とみなされ、期待される結果を生み出す。取引出力は大多数のネットワーク参加者により有効な子取引と関連づけられた際に「使用済み」とみなされ、大多数のネットワーク参加者により有効な子取引と関連づけられていないとみなされた場合は「未使用」と考えられる。取引の出力の「所有権」や「権利」という概念はどのエンティティが前記の出力を制御するか、より具体的に言うと、誰が新しい取引を作成または大多数のネットワーク参加者に有

効だと認められるように出力を「使用」させるかということにより定義される。
【００１０】
より具体的に言うと、新しい取引を元帳に提出しようとしているエンティティは所望の取引の詳細を含む取引記録を知り合いの複数のネットワーク参加者（「ピア」と呼ばれる）に発信（または「放送」）するのである。これらのピアたちはそれぞれに取引記録の検証を試み、成功した場合には取引記録を更に彼らのピアに発信し、そのように続いていく。最終的に取引記録はその取引を含むことでその取引を実行するように構成された参加者に届くようになっている。
【００１１】
あるエンティティが大多数によって有効であるとして受け入れられた子取引を生成し、その入力が親取引からの未使用の出力に関連づけられている場合に取引が行われる。殆どの場合、これは第二のエンティティへの単純な制御の移動であり、新しい取引の出力スクリプトは、対応する入力スクリプトを作成することは特定の非対称グリッド・キー・ペアを所有する単一のエンティティにとって計算上簡単であり他のすべてに対して計算的に非実用的である小さな一連の操作である。言い換えると、特定のプライベートキーへのアクセスを持つエンティティにアドレス化される。既存のソフトウェアはこれらのアドレスや簡単な取引をプログラマーやプロトコルの専門家ではない一般的な人のために抽象化している。
【００１２】
しかし、取引が有効であると受け入れられる条件として記述されるスクリプトは一連の利用可能な操作によって考慮されている。これらの操作を記述する一般的な方法はふつうバイナリーまたはプログラミングコードであるために（非特許文献３）、一般人には任意の取引を作成したり理解したりすることはできない。例えば、２０１４年４月２１日現在では、Ｂｉｔｃｏｉｎ　Ｃｏｎｔｒａｃｔｓ　Ｗｉｌｄページはいくつかの理論上の簡単な説明で構成されている（非特許文献４）。それぞれは取引における役割には関係なく、一般人にはこれらの指示を理解することすら難しい。類似する取引を自信を持って行うための基本的なステップやそういった取引のコンビネーションが欠如している。大きな可能性を秘めているものの、抽象化されていないこの種の複雑性はビットコインプロトコルやその派生がこれまでの「簡単な」支払い方法のように普及することの妨げになっている。
【００１３】
分散型デジタル通貨または「仮想通貨」
【００１４】
ビットコインプロトコルとその派生のデザイン及び機能は以下のように説明することができる（非特許文献５）。このセクションはビットコインをその名前で言及するが、この説明は当技術分野で現在知られているほぼ全ての分散型デジタル　通貨に共通して正しいと言える。
【００１５】
ブロックチェーン：「ブロックチェーン」とはビットコインの取引を記録する公共の元帳である。新しいソリューションではブロックの維持を中央権威の介入なしで達成することができる。連鎖はビットコインソフトウェアを実行する通信ノードを経由する通信ネットワークにより実行される。「支払人Ｘがビットコインを受取人Ｚに送信する」形式の取引は、簡単に利用可能なソフトウェアアプリケーションを使用してこのネットワークにブロードキャストされる。ネットワークノードは取引を検証し、それを元帳のコピーに追加し、これらの元帳追加を他のノードにブロードキャストすることができる。あらゆるビットコイン額の所有権を独立して検証するために、各ネットワークノードはブロックチェーンの独自のコピーを保管する。１時間につき約６回、受け入れられた取引の新しいグループ（ブロック）が作成、ブロックチェーンに追加された直後にすべてのノードに公開される。これにより、ビットコインソフトウェアは、特定のビットコインがいつ使われたかを判断することができる。これは中央権威なしの環境での二重支出を防ぐために必要である。従来の元帳は、実際の請求書またはそれとは別に存在する約束手形の移転を記録するの

に対して、ブロックチェーンは、ビットコインが未使用の取引出力の形で存在すると言える唯一の場所である。

【００１６】

単位：ビットコインの会計単位はビットコイン（）である。代替単位として利用されるビットコインの小さい倍数はミリビットコイン（ｍＢＴＣ）ミクロビットコイン（μＢＴ）及びサトシである。ビットコインの作成者にちなんで名付けられた「サトシ」はビットコインの最小倍数で、０．００００００００１、つまり一億分の１ビットコインを表す。ミリビットコインは０．００１ビットコイン、つまり千分の１ビットコイン、ミクロビットコインは０．０００００１ビットコイン、つまり百万分の１ビットコインを表す。ミクロビットコインは「ビット」とも呼ばれる。

【００１７】

所有権：図２４参照　ビットコインの所有権とはユーザーが特定のアドレスに関連づけてビットコインを使用できることを表す。そのためには支払う側が個人のキーを使い取引にデジタル署名をする必要がある。個人キーの知識がなければ取引は署名されずビットコインも使えない。ネットワークは公共キーを使い署名を確認する。個人キーを紛失した場合、ビットコインネットワークはそれ以外のいかなる所有権の証拠も認識しない。したがってコインは使用不可となり、実質的に失われる。２０１３年には個人キーを保存していたハードドライブを捨ててしまった際に７，５００ビットコインを失くした（時価７５０万ドル）と言ったユーザーもいた。

【００１８】

取引：通常、取引とは一つ以上の入力を必要とする。（「コインベース」はビットコインを作成するための特別な取引で入力は０である。後述の「マイニング」及び「供給」を参照）取引が有効であるためには全ての入力は以前の取引の「未使用の」出力でなければならない。そして全ての入力はデジタル署名を必要とする。複数の入力は現金取引での複数のコインの使用を意味する。取引は複数の出力を持つこともでき、一回で複数の支払いをまとめてすることもできる。取引の出力は任意の「サトシ」の倍数として指定できる。現金取引と同様に、入力合計（支払いのためのコイン）は支払い金額の合計以上とすることもできる。そのような場合、追加の出力によりお釣りが支払う側に戻って来る。取引の出力に含まれないサトシの入力が取引手数料となる。

【００１９】

全ての取引記録には「ロックタイム」が付随する。これは取引が有効であると受け入れられることを防ぎ、合意された将来のある時点まで取引が保留もしくは交換可能とする。ビットコインや類似のプロトコルではブロックインデックスもしくはタイムスタンプとして指定できる。ロックタイムに到達するまで取引記録はブロックチェーンには受理されない。他のより柔軟性のあるメカニズムも提案されている（非特許文献６）。

【００２０】

マイニング：「マイニング」とは記録管理サービスである。マイナーはブロックチェーンを繰り返し検証すること、新しく発表された取引を「ブロック」と呼ばれる新しい取引グループに収集することでブロックチェーンを一定で完了、不変に保つ。新しいブロックは前のブロックに「繋がる」情報を保有している。（それが名前の由来である）その情報はＳＨＡ－２５６ハッシュタグアルゴリズムを利用した前のブロックの暗号ハッシュである。

【００２１】

新しいブロックにはいわゆる「プルーフ・オブ・ワーク」が含まれている必要がある。プルーフ・オブ・ワークには「難易度の目標」と呼ばれる数字と、専門用語である「ｎｏｎｃｅ」、つまり一度だけ使用された数字が含まれている。マイナーは難易度の目標に示されているより小さい新しいブロックのハッシュを生成する「ｎｏｎｃｅ」を見つけなければならない。新しいブロックが作成されてネットワークに配信される時には、ネットワークノードは簡単に証明を検証できる。一方で安全な暗号ハッシュに必要な「ｎｏｎｃｅ」を見つけるには一つしか方法がないため、証明を見つけるのは相当な仕事である。その

方法とは必要な出力が獲得されるまで１、２、３、と異なる整数を一つずつ試すことである。新しいブロックのハッシュは困難度の目標より小さいということは、この面倒な作業が実際行われているということを証明することが「プルーフ・オブ・ワーク」と呼ばれている所以である。

【００２２】

ブロックを繋ぐこととプルーフ・オブ・ワークシステムは、一つのブロックが受け入れられるには攻撃者は全ての後続のブロックを修正する必要があるために、ブロックチェーンの変更を極めて困難にしている。新しいブロックは常に掘り起こされているため、時間が経てばたつほど後続のブロック（与えられたブロックの確認とも呼ばれる）の数も増え、ブロック変更の難しさも増す。

【００２３】

供給：新しいブロックを見つけることに成功したマイナーは、新しく作成されたビットコインと取引手数料によって報酬を受ける。２０１２年１１月２８日の時点では、ブロックチェーンに加えられた各ブロックにつき報酬は２５の新しく作成されたビットコインだった。報酬を受けるための「コインベース」と呼ばれる特別な取引が処理された支払いに含まれている。出回っている全てのビットコインはそのコインベース取引まで遡ることができる。ビットコインプロトコルはブロックを追加する報酬は約４年ごとに半減すると指定している。最終的には任意の制限である２１４０年ごろに２１００万ビットコインが出回った時には報酬自体が廃止され、記録管理は取引手数料のみで報酬を受けることになる。

【先行技術文献】

【非特許文献】

【００２４】

【非特許文献１】電子取引、Ｒｏｓｅ，　Ｄａｖｉｄ　Ｃ．　経済行動における道徳的基盤、ニューヨークＯｘｆｏｒｄ　ＵＰ，　２０１１年　印刷、高価な手数料を払い第三者を使用した「オンライン」エスクロー及び紛争解決、様々な評判システム、第三者保証人など。

【非特許文献２】これはビットコインプロトコルを過度に簡略化した説明である。詳細な情報はビットコインウィキ＜ｈｔｔｐｓ：／／ｅｎ．ｂｉｔｃｏｉｎ．ｉｔ／＞を参照。Ｅｔｈｅｒｅｕｍプロトコルに関する詳細な情報はＥｔｈｅｒｅｕｍウィキ＜ｈｔｔｐｓ：／／ｇｉｔｈｕｂ．ｃｏｍ／ｅｔｌｉｅｒｅｕｍ／ｗｉｋｉ／ｗｉｋｉ＞参照。元帳記録（すなわち有効な「ブロック」については下記の詳細な説明を参照）

【非特許文献３】「ビットコイン　マルチシグネチャー２－ｏｆ－３取引の作成方法」を参照　ＳｔａｃｋＥｘｃｈａｎｇｅ　２０１４年3月２３日　ウェブ　２０１４年４月。ｈｔｔｐｓ：／／ｂｉｔｃｏｉｎ．ｓｔａｃｋｅｘｃｈａｎｇｅｘｏｍ／ｑｕｅｓｔｉｏｎｓ／３７ｉ２／ｈｏｗ－ｃａｎ－ｉ－ｃｒｅａｔｅ－ａ－ｍｕｌｔｉ－ｓｉｇｎａｔｕｒｅ－２－ｏｆ－３－ｔｒａｎｓａｃｔｉｏｎ）

【非特許文献４】ハーン、マイク　「契約」ビットコイン　ビットコインコミュニティ　２０１４年４月9日　ウェブ２０１４年４月＜ｈｔｔｐｓ：／／ｂｉｔｃｏｉｎ．ｓｔａｃｋｅｘｃｈａｎｇｅｘｏｍ／ｑｕｅｓｔｉｏｎｓ／３７ｉ２／ｈｏｗ－ｃａｎ－ｉ－ｃｒｅａｔｅ－ａ－ｍ　ｕｌｔｉ－ｓｉｇｎａｔｕｒｅ－２－ｏｆ－３－ｔｒａｎｓａｃｔｉｏｎ＞。

【非特許文献５】＜ｈｔｔｐｓ：／／ｅｎ．ｗｉｋｉｐｅｄｉａ．ｏｒｇ／ｗｉｋｉ／Ｂｉｔｃｏｉｎ＞及び＜ｈｔｔｐｓ：／／ｅｎ．ｂｉｔｃｏｉｎ．ｉｔ／ｗｉｋｉ／Ｃｏｎｔｒａｃｔｓ＞からの引用。）

【非特許文献６】例「ＢＩＰ－６５：Ｒｅｖｉｓｉｔｉｎｇ　ｉ　ＬｏｃｋＴｉｍｅ」Ｑｎｔｒａ．ｎｅｔ、２０１４年１１月１３日。ウェブ２０１５年５月４日　＜ｈｔｔｐ：／／ｑｎｔｒａ．ｎｅｔ／２０１４／１１／ｂｉｐ－６５－ｒｅｖｉｓｉｔｉ１１ｇ－ｎｉｏｃｋｔｉｍｅ／＞。

【発明の概要】

【００２５】
本発明は基礎となる転送メカニズムに関する特別な技術的知識がなくても、任意の距離で、第三者の入力を条件とした合意を取り決め強制させるに関連するものであり、随意に第三者の介入、譲渡人及び譲受人の代理、期間の置き換え、改訂、改善などができるシステムやメソッドに関連するものである。このような転送がこれまでは必要であった高額の第三者仲介人を介さずに、またこれまでのような取引先リスクなしに確実に行うことができる。
【００２６】
このアプリケーションでは、任意のスワップと信用状という二つの価値転送形式について考察する。任意のスワップや信用状は二つとも全く異なるものであるため例証に有用である。しかし、この発明により著しく類似した表現や強制力をもつ。この発明が他の多くの価値転送にも活用できることは当事者には理解できるだろう。
【００２７】
一例では、ビットコインがニュージーランドドルで評価された場合これから数週間の間にかなり価値が上昇するとＡが考えているとする。そしてＢはその逆、つまりビットコインがニュージーランドドルで評価された場合これから数週間の間に価値が下落すると考えている。どちらもお互いのことは知らないが、かれらの信念に沿った小さい賭けをしてみたいと考えている。本発明の一実施形態では両者が互いを見つけ出し、具体的な条件を決めるために協議し、いままでの高額な方法を抜きにこの合意を強制することを可能にする。
【００２８】
また別の例では、Ａはサービスへの支払いをビットコインでも可能にしたいと考えている商売人だが変動しやすいビットコインよりは米ドルで支払いを受けたいとも思っている。彼女はビットコインの米ドルに対しての価値の上下は気にならない。定期的に（１日一回、もしくは取引のたびに）米ドルで評価されたビットコインのエクスポージャーを顧客から受け取るビットコインに比例して販売することができる。言い換えると、ビットコインのエクスポージャーを米ドルと換金する。Ｂはビットコインが欲しいけれど米ドルを多く持っていて、米ドルで評価されるビットコインのエクスポージャーをより多く欲しいと思っている。本発明の一実施形態として、ＢがＡを見つけ出し、Ａとエクスポージャーを交換またはスワップすることを可能にし、またもしビットコインの価値が米ドルに対して下がったとしても、ビットコインの価値が米ドルに対して上昇した時にＢがその上昇分を受け取るという条件で、Ｂが補填してくれるのでＡが商品やサービスの支払いをビットコインで受け取ることも可能にしている。他の実施形態ではこれらのスワップをＡが追加のビットコインを受け取ったと感知されるたびに、自動に探し出す。
【００２９】
組み合わせが可能である。たとえばＡは豪ドル（ＡＵＤ）を受け付けるが米ドルを好み、豪ドルが米ドルに対して持つ変動性をリスクヘッジしたいと考えている。本発明の一実施形態ではＡが米ドルのエクスポージャーをビットコインでＢと交換し、ビットコインのエクスポージャーをＣと豪ドルで同様の期間に交換すれば、豪ドルのリスクヘッジを米ドルで合成することができる。ＢとＣが違った主体でなくてもよく、（同一人物だということもありえる）Ａが二つの異なる取引をしなくても良い。更に本発明の様々な実施形態は、当事者が外貨預金の維持または通貨の購入、交換を行うことなくこの種の取引を実行することを可能にする。
【００３０】
更に別の例では、Ａがお互いによく知らないＢから商品を購入したい場合ＢはＡからの資金の利用可能性の保証を望むが、ＡはＢが出荷の証拠を示す（及び他の所定の条件を満たす）までＢ（または譲渡人）にそれらの資金を解放したくないという場合がある。
【００３１】
スワップを含む一つの実施形態では「クライアント」と呼ばれる一つ目の装置と二つめのクライアントが、第一のクライアント、第一のクライアント、もしくは仲介者のうちの

いずれか二人が結託して、ある特定の期間における金融商品の相対価値などといった仲介者による外部状態の観察に基づいた計算により第一の当事者の資産（例えば未使用の取引出力など）と第二の当事者の資産が解放されるまではそれらの資産はコミットされたままであるというような一連の取引に参加する場合もある。

【００３２】

信用状に関連する他の実施形態では、第一と第二のクライアントが、荷主やある住所への配送の検証など外部状態の観察に基づき第一のクライアント及び仲介者が第一のクライアントの資産を解放するまでコミットされたままであるという一連の取引に参加する場合もある。

【００３３】

さらなる実施形態では、そのような観察が見られない場合有効期限のタイムスタンプによって資産は返金される場合もある。

【００３４】

別の実施形態では、仲裁役によって円滑に和解が決まるまで資産のコミットメントは延期される場合もある。

【図面の簡単な説明】

【００３５】

【図１】図１はクライアント（１２０、１６０、１７０）、転送メカニズム（１１０，１５０）、ファシリテータ（１００）、データソース（１３０）といった異なる参加者がコンピューターネットワーク（１４０）により繋がっている分散型のデジタル通貨（１５０）などの転送メカニズムを使用及び含んでいる本発明の典型的な実施形態である。

【図２】図２は一つ以上のソース取引、コミット取引を含むスワップに関係する一実施形態の側面を示している。

【図３】図３はコミット取引、返金取引を含むスワップに関係する一実施形態の側面を示している。

【図４】図４から図５は元本及び担保を含む比較的単純なスワップに関係する一実施形態の側面を示している。

【図５】同上。

【図６】図６から図７は当事者の片方が終了以前に離脱したいと望むが相手の合意を保証できていない場合に、それでも離脱したい当事者の代わりになる意思を持つ第三者を見つけた場合の複数のスワップ実施形態例からの取引チェーンを示している。

【図７】同上。

【図８】図８はソース取引、コミット取引を含む信用状に関連する一実施形態の側面を示している。

【図９】図９はコミット取引、有効期限取引を含む信用状に関連する一実施形態の側面を示している。

【図１０】図１０及び図１１は元本及び担保を含む比較的単純な信用状に関係する一実施形態の側面を示している。

【図１１】同上。

【図１２】図１２から１４は当事者の入れ替わりを含む信用状に関係する複数の実施形態例からの取引チェーンを示している。

【図１３】同上。

【図１４】同上。

【図１５】図１５及び図１６は価値転送の当事者が紛争時のために仲介者を設定した場合の実施形態の側面を示している。

【図１６】同上。

【図１７】図１７～図２２は一実施形態内で価値転送を行う主要な段階を示している。

【図１８】同上。

【図１９】同上。

【図２０】同上。

【図２１】同上。
【図２２】同上。
【図２３】図２３は、クライアント（１２０）またはファシリテータ（１００）を含む典型的な実施形態の構成要素を示す。
【図２４】図２４（従来技術）は分散型デジタル通貨での所有権の簡素化されたチェーンを示している。
【発明を実施するための形態】
【００３６】
本発明は、以下の実施形態に限定されるものではない。以下の説明は例示のためであり、限定されない。他のシステム、方法、特徴および利点は図面および詳細な説明の検討の際に当業者に明らかになるだろう。すべてのそのような追加のシステム、方法、特徴、および利点は、本発明の主題の範囲内であり、この説明内に含まれ、そして添付の特許請求の範囲によって保護される意図にある。
【００３７】
例えば、ビットコインプロトコルは、多くの場合、例示の手段として、本出願において使用されるが、本発明は特にビットコインプロトコルに限定されるものではない。特定の厳密に定義された基準が満たされない限り、資産（仮想またはそれ以外）の所有権を再び特徴付けることを十分に困難にする技術を代用することができる。本発明は分散型又は集中型の転送メカニズムに限定されるものではない。例えば、一実施形態において、権限（集中型）によって認識（すなわち円滑化）されることもできれば、別の実施形態では選挙（分散型）等によって確認することができる、など。
【００３８】
更に、ビットコインプロトコルと同様の技術は取引において明示的に「入力」と「出力」を識別するが、本発明はこのような転送メカニズムに限定されるものではない。転送メカニズムは必要な機能を公開しているとすると、資産の所有権を再分類することができる任意の文脈で本発明の様々な実施形態を実施することができる。このアプリケーションは、「入力」と「出力」という言葉を文字通り（ビットコインやその派生のテクノロジーについてなど）及び比喩的に（複式簿記、権原連鎖などの他のテクノロジーなど）使う。より伝統的なモデルでは、例えば、「入力」とはある事業体の制御のもとにある口座の利用可能な「残高」の一部及び全部を意味していた。（伝統的な銀行など）そして「出力」とは例えば他の事業体の口座（口座番号など）への言及を含んでいて、そのようなモデルでは資産の再分類は所定の条件が満たされ次第、第一の事業体の口座が減額され、第２の事業体の口座の残高が（なるべく微小に）第二の事業体の口座が増額される。これは本発明が実施される可能性のある代理の転送メカニズムの一例でしかない。
【００３９】
更に本出願は、「ディスプレイ」、「ユーザー入力」、「表示デバイス」、「ユーザー入力装置」などといった用語を使って本発明の内容の開示または暗示する可能性がある。しかしながら本発明は一般的五感能力を有する者によって実施されることに限定されるものではなく、「ディスプレイ（装置）」は感覚もしくは感覚の組み合わせのいずれかを介して明確に人間に情報を通信することができる装置を含むことが意図される。例えば、盲人はテキスト音声合成器を含む「オーディオ・ディスプレイ」を持つ装置及び点字端末を使用することができる。同様に、ユーザー入力（装置）とは人間からの情報を受信することができる任意のデバイスを含むことが意図される。ＭｏｄｅｒｎＳｙと呼ばれる人気のユーザー入力装置は、キーボード、マウス、タッチスクリーン等を含むだけでなく、音声合成器、息操作デバイス、クリックアンドタイプデバイス、動き又はジェスチャー認識装置でもある。これらはほんの数例だ。そのようなディスプレイおよびユーザー入力装置の多様性は、当該分野で公知であり、もちろん本発明を実施する際に使用することができる。
【００４０】
図１に示す実施形態では、本発明はコンピュータネットワーク上の図示された参加者の

一部または全部を含む。参加者は典型的にコンピュータネットワークに接続された第一の当事者（図示せず）のために動作する第一のクライアント（Ａ）、持続的または間欠的にコンピュータネットワークに結合された第二の当事者（図示せず）、コンピュータネットワークを介してアクセス可能な転送メカニズムと、コンピュータネットワークにアクセス可能なファシリテータと、任意選択でファシリテータによってアクセス可能な一つまたは複数のデータソースとを含む。典型的な実施形態では、コンピュータネットワークはインターネットおよび関連技術を含むが、これは必要条件ではない。他の構成も可能である。例えば、コンピュータネットワークは、プライベートネットワーク、ＶＰＮ、セキュアトンネル、フレームリレーなど、参加者の任意のサブセットに接続するための複数の独立したコンピュータネットワークを含むことができる。非限定的な最新機器の例には、ハードワイヤ、ファームウェア、ソフトウェア、そして一緒に使用されるイーサネット、無線イーサネットＴＭ（Ｗｉ－Ｆｉ）、モバイル無線（例えばＣＤＭＡ、ＦＤＭＡ、ＳＯＭＡ、ＴＤＭＡ、ＧＳＭＴＭ（ＧＲＰＳ）、ＵＭＴＳ、ＥＤＧＥ、ＬＴＥなど）ブルートゥース（登録商標）、ファイヤーワイヤー、ＵＳＢ、ＩＰ、ＴＣＰ、ＵＤＰ、ＳＳＬなどのような他のネットワーク技術を使用してもよい。

【００４１】

典型的な実施形態では、第一のクライアント、第二のクライアントとファシリテータの各々は、本発明の範囲内の特定のステップを実行するように構成されたコンピュータプロセッサを備える。このような転送メカニズムとしてＥｔｈｅｒｅｕｍプロトコルを使用するもののようないくつかの実施形態では、ファシリテータは、プルーフ・オブ・ワークプロトコルによりネットワーク参加者が評価される計算の命令を含み、この場合、ネットワーク参加者は、計算のために命令を評価するように構成されたコンピュータプロセッサを備える。多くの実施形態では、クライアントは人間と対話するためのディスプレイ装置と入力装置を備えるが、これは厳密に必要ではない。他の実施形態ではクライアントは人の介入を必要とせず完了に自動化することができる。このような一実施形態では、第一のクライアントのコンピュータプロセッサは、転送メカニズム、ファシリテータ、データソース、第二のクライアントなどまたはいくつかの他の入力の状態を監視するように構成されており、また状態変化に基づいて様々な参加者と自動的に相互作用するように設定されている。

【００４２】

例えば、一実施形態での転送メカニズムはビットコインプロトコルを含み、各クライアントおよびファシリテータはキーペアや第一の取引を補完するための固定的データストアを備えている。第一のクライアントはビットコインの新しい所有権を取得したことを観察すると、ファシリテータを介してある金融商品や証券（米ドルなど）のエクスポージャーへの交換と引き換えに別の金融商品や証券（ビットコインなど）のエクスポージャーを取引するオファーを開始するように設定されている。

【００４３】

図１は、クライアント、転送メカニズム、ファシリテータ、およびデータソースが別個の参加者であり、特に分散転送メカニズムと共に使用するための典型的な本発明の実施形態を示す。しかしながら、図示された構成は、本発明によって企図される唯一の構成ではない。別の実施形態では、ファシリテータは、転送メカニズムのいくつかまたは全ての態様を示している。別の実施形態では、ファシリテータは、クライアントのいくつかまたはすべての態様を含む。例えばクライアントのデータストアの一部または全部や、オファーを開始または受け入れる能力などはファシリテータに「埋め込まれる」ことができ、それによってファシリテータがクライアントを代表することが可能になる。（例えばファシリテータの所有者によって制御されるもの、またはファシリテータへ支配権を委任した第三者の代わりとして）さらに別の実施形態では、ファシリテータは、データソースを備える。本発明によって企図される多くの構成が可能であり、当業者には明らかになるであろう。

【００４４】

図２は、一つまたは複数のソース取引およびコミット取引を含むスワップに関する一実施形態の態様を示す。　図示のように、コミット取引は第一のソース取引（すなわち、第一の当事者）から第一の量を受け入れるための第一の入力と、第二のソース取引から（すなわち、第二の当事者から）第二の量を、そしてこれらの量の部分を一つ以上の他の取引（図示せず）に向けるための一つ以上の出力を備えており、多くの場合第一及び第二の量は同等であるが必ずしもそうではなく、場合によっては複数の図に示されているように元本額の（Ｐ）および（任意の）担保量（Ｃ）を含む予想される量の合計である。

【００４５】

典型的な実施形態では、コミット取引はその出力（複数可）を介して利用可能金額の一部または全部が第一及び第二の当事者、ファシリテータ、そして任意の第三者のうちの少なくとも二者から確認ができて初めて使用できる。他の実施形態では、コミット取引は、その出力を介して利用可能な金額の一部または全部がファシリテータか任意の信頼できる第三者のうち一人と、第一及び第二の当事者のうち一人の確認をもって初めて使用できるように構成されている。別の実施形態のコミット取引は、その出力を介して利用可能な金額の一部または全てが第一の当事者又は第二の当事者、第三の当事者、および任意選択で必要に応じて信頼できる第三者のいずれかから確認して転送することができるように構成されている。これらは非限定の例であり、ここで提示された例に加えてコミット取引は出力が人数を問わず所有権を確定するように設定されても良い。これらの取引は権限のある当事者によって署名されなければならない当座預金口座にいくらか類似しているといえる。

【００４６】

第一のソース取引と第二のソース取引が図２に示されているが、これは本発明を限定するものとして解釈されるべきではない。金額は任意の数の異なるソースからのコミット取引に入力される可能性がある。超過分は完了に元の、または異なる当事者に返金される。唯一の制限は、コミット取引が、少なくともいくつかの実施形態では、それぞれのソースから前記入力に金額を送るために課される料金（図示せず）を補うためにコミット取引を調整する必要がある。例えば転送メカニズムは、転送料、引き出し手数料、電信料などを課す可能性がある。例としてビットコインプロトコルでは、ブロックチェーンでのタイムリーな取引を保証するために「マイニング料金」が必要な場合がある。

【００４７】

図３は、コミットを含むスワップに関する一実施形態の態様を示す。取引および払い戻し取引を含む。コミット取引は、第一元本量（P_A）を受信するための第一入力、第二元本量（P_B）を受信するための第二入力、およびコミット出力を含む。払い戻し取引ではコミット出力から金額を受け取るための入力と、第一当事者への第一返金出力、第二当事者への第二返金出力とを含む。典型的な実施形態では、払い戻し取引記録はコミット取引の一定期間後に生成されるか、または将来の一定時間後にコミット出力がまだ使用いない場合にのみ有効であるように生成される。これにより、別の取引優先的にコミット出力を使用することが可能であり、そのような他の取引が作成されていない場合は払い戻し取引記録を転送メカニズムに送信して、当事者を元の立場に戻すこともできる。

【００４８】

図４－５は、元本及び担保を含むスワップ状況における比較的単純な支払い取引を含むスワップ実施形態の態様を示す。図２―図４に示すように、コミット取引は、第一当事者からの第一の元本及び担保入力、および第二当事者からの第二の元本および担保入力を含む。図２　図５に示すように、コミット取引は、第一当事者からの第一元本（P_A）、第一当事者からの第一担保（C_A）、第二当事者からの第二元本入力（P_B）、および第二当事者からの第二担保（C_B）から構成される。これらは当業者には明らかになるであろう多くの可能な構成のうちの二つに過ぎない。例えばコミット取引は、第一当事者からの元本入力、第二当事者からの担保入力（例えば、図示していない第一当事者の保証人）、及び第三者からの元本及び担保入力を含むことができる。

【００４９】

図４および図５に示す実施形態では、各支払い取引はコミット出力から金額を受け取るための入力を含む。図４では第一当事者への修正された元本及び担保支払い出力、第二当事者への修正された元本及び担保支払い出力、及び任意の第三当事者への手数料（φ）出力を含む。図５では支払い取引は、第一当事者への担保支払い出力、第一当事者への修正された元本支払い出力、第二当事者への変更された担保支払い出力、および第三者への任意の手数料出力を含む。これらは、当業者には明らかになるであろう多くの可能な構成のうちの２つにすぎない。　例えば、上記と同様に支払い取引は、第一当事者への修正された元本支払い出力、第三当事者（例えば、第一当事者の保証人）への修正される可能性のある担保支払い出力（元本が枯渇した場合）、もしくは第二当事者への修正される可能性のある担保支払い出力（元本が枯渇した場合）で構成される場合もある。

【００５０】

図４および図５に示す実施形態では、手数料は修正された元本から配分され取引の当事者間で均等に分配されるがこれは必須ではない。手数料は任意の段階、または複数の段階で割り振ることができる。それは当事者の一人が全てまたは多い割合を負担することもできる、また、図４および図５に示す各実施形態において、複数の支払い出力の金額の計算は、ある当事者にとってプラスであり、他の当事者に負である差（δ）を含む。図５に示す支払い取引において例えれば、第二の元本がスワップの有効期限前に使い尽くされると担保からの金額の配分が必要である。言い換えれば：

【数１】

$$\delta > P_B - \frac{1}{2}\varphi \qquad [\text{eq. 1}]$$

【００５１】

基本的なスワップ契約を円滑化するために上記の様々な構成要素のいくつかを使用できる。その方法を例示するために、当事者同士が互いに信頼しておらず、ファシリテータもいずれの当事者によっても完了に信頼されていない状態でのビットコインまたは同様のプロトコルの転送メカニズムで、以下のステップが一実施形態内で起こると仮定する。

１．第一のクライアントが以下の条件を備えるオファーを送信する。条件とは、以下のものを含む。

（ａ）基本の証券及び見積もり証券とのうちの少なくとも一つを含むデータソースへの参照、

（ｂ）元本額、

（ｃ）有効期限のタイムスタンプ、

（ｄ）任意選択で名義資産への参照、

（ｅ）任意選択で担保金額、

（ｆ）任意選択で支払い機能。

例えば以下のように表現できる。

【表１】

Example terms:

Base: USD

Quote: AUD

Denominating: BTC

Principal: 0.5 (BTC)

Collateral: 2 × principal

$res_{base}(b_o, q_o, b_f, q_f)$: $principal \times \frac{b_f - b_o}{q_f - q_o}$

Expiration: 2014-06-01T12:34:56Z

２．任意選択でファシリテータはオファーの態様（例えば、ファシリテータが用語を解釈できる、有効期限が許容範囲内にあるなど）を検証する。検証が認められない場合、ファシリテータはオファーを拒否することができ、任意選択でエラーメッセージを第一のクライアントに送信することもできる。
３．第二のクライアントは、ファシリテータからオファーを回収する。
４．第一のクライアントは、転送メカニズムへの取引ＩＤを含む第一のソース取引記録を作成する。
５．第二のクライアントは、転送メカニズムへの取引ＩＤを含む第二のソース取引記録を作成する。
６．第二のクライアントは、第二のソース取引記録の取引ＩＤを任意選択でファシリテータを介して第一のクライアントに送信する（例えば同じメッセージ内で、オファーＩＤ、オファーハッシュ等を介して）。別の実施形態では、第一のクライアントは、第一のソース取引記録の取引ＩＤを第二のクライアントに送信し、その後のステップは、この実施形態の以下を反映する。
７．第二のクライアントおよびファシリテータのうちの一人は、第二のパブリックキーを、オファーに関連付けられた方法で第一のクライアントに送信する。
８．第一のクライアントは、完了コミット取引記録を作成するために、未完了のコミット取引記録の第一の元本入力に署名（すなわち、暗号署名を計算してそれに関連付け）する。未完了のコミット取引記録は、以下のものを含む。
（ａ）第一のソース取引から第一の元本金額を受け取るための第一の元本入力、
（ｂ）第二のソース取引から第二の元本金額を受け取るための第二の元本入力コミット額
（ｃ）（ｉ）第一のパブリックキー、（ｉｉ）第二のパブリックキー、（ｉｉｉ）ファシリテータのパブリックキーのうちの二つのプライベートキーの署名を必要とすることを条件に含むコミット出力。
未完了のコミット取引記録の例：

【表２】

```
Input:

      Previous tx: 85e5...e61f

      Index: 1

      scriptSig: efd6...ea1601 a6a6...2c2b

Input:

      Previous tx: 705d...9ce2

      Index: 0

      scriptSig: [sig. placeholder]

...

Output:

      Value: 300000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

９．第一のクライアントは、場合によってはファシリテータを介して、第二のクライアントに未完了のコミット取引記録を送信する。ファシリテータは任意選択で初期コミット取引記録の態様（例えば、初期コミット取引記録が第一当事者によって署名され、第一元本額および第二元本額がそれぞれ条件を満たしているなど）を検証する。検証が認められなかった場合、ファシリテータは第一のコミット取引を拒否することができ、場合によっては第一のクライアントにエラーメッセージが表示される。ファシリテータは任意選択で第二のクライアントにオファーおよび初期コミット取引記録を送信する。

１０．第二のクライアントは任意選択で未完了のコミット取引記録が第一の当事者によって署名されたかなどを検証する。

１１．第二のクライアントは未完了のコミット取引記録に署名することによって完了コミット取引記録を作成し、任意選択で固定メモリに保存する。完了コミット取引記録には、以下のものを含む。

（ａ）第一の原本取引から第一の元本金額を受け取るための第一の元本入力、

（ｂ）前記第二のソース取引から第二の元本金額を受け取るための第二の元本入力、

（ｃ）コミット額と（ｉ）第一のパブリックキー（ｉｉ）第二のパブリックキー。（ｉｉｉ）ファシリテータのパブリックキーのうちの二つのプライベートキーの署名を必要とすることを条件に含むコミット出力。

完了コミット取引記録の例：

【表３】

```
ID: 6b24...b607

Input:

      Previous tx: 85e5...e61f

      Index: 1

      scriptSig: efd6...ea1601 a6a6...2c2b

Input:

      Previous tx: 705d...9ce2

      Index: 0

      scriptSig: 78eb...fc4501 531f...00dd

...

Output:

      Value: 300000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

１２．第二のクライアントは、以下のものを含む未完了の払い戻し取引記録に署名する。
（ａ）有効期限タイムスタンプ後のロックタイム、
（ｂ）コミット取引記録からコミット額を受け取るための入力、
（ｃ）第一の払い戻し額と、第一当事者の承認を必要とする第一の条件を含む第一の払い戻し出力、
（ｄ）第二払い戻し額と、第二の当事者の承認を必要とする条件とを含む第二の払い戻し出力。
未完了の払い戻し取引の例

【表４】

```
Input:

      Previous tx: 6b24...b607

      Index: 0

      scriptSig: OP_0 [sig. placeholder] c255...d80301

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

１３．第二のクライアントは第一のクライアントに場合によってはファシリテータを介して、完了コミット取引記録および未完了の払い戻し取引記録を送信する。ファシリテータは任意選択で完了コミット取引記録および未完了の払い戻し取引記録を検証する。（例えば第一当事者および第二当事者によって完了払い戻し取引記録が署名されているか、未完了の小切手の払い戻し取引記録が第二当事者によって署名されているか、未完了の払い戻し取引記録と完了コミット取引記録額の記述が同等であるか、未完了の払い戻し額が第一元本額以下であること、小額払い戻し取引記録の第二払い戻し額が第二元本額以下であること、ロックタイムが有効期限のタイムスタンプの後であることなど）妥当性の検証が認められなかった場合、ファシリテータは払い戻し取引記録または完了コミット取引記録を拒否することができ、任意選択で第二のクライアントにエラーメッセージを送ることもできる。ファシリテータは任意選択で、完了コミット取引記録および未完了の払い戻し取引記録を第一のクライアントに送信する。

１４．第一のクライアントは任意選択で完了コミット取引記録が期待通りであり、第一の当事者および第二の当事者によって署名されたこと、初期払い戻し取引記録が期待通りであり、第二の当事者によって署名されたこと等を確認する。

１５．第一のクライアントは任意選択で完了コミット取引記録のコピーを固定メモリに保存する。

１６．第一のクライアントは任意選択で完了払い戻し取引記録を作成し、そのコピーを固定メモリに保存する。完了払い戻し取引記録には、

（ａ）有効期限タイムスタンプ後のロックタイム、

（ｂ）完了コミット取引からコミット額を受け取るための入力、

（ｃ）第一の払い戻し金額と第一の当事者の承認を必要とする第一の条件を含む第一の払い戻し出力と、第二払い戻し金額と、第二当事者の承認を必要とする条件を含む第二払い戻し出力、

が含まれている。
完了払い戻し取引記録の例
【表５】

```
ID: d5f8...8ab5

Input:

      Previous tx: 6b24...b607

      Index: 0

      scriptSig: OP_0 b859...452c01 c255...d80301

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

１７．第一クライアントは、場合によってはファシリテータを介して、第二のクライアントに完了払い戻し取引記録を送信する。ファシリテータは任意選択で完了払い戻し取引記録の態様を検証する（例えば、両方の当事者によって署名されていること、完了払い戻し取引記録が他の方法で修正されていないこと、完了コミット取引記録の条件と同様であることなど）。検証が失敗した場合、ファシリテータは、完了払い戻し取引の記録を拒否するか任意選択で第一のクライアントへエラーメッセージを送信することができる。ファシリテータは任意選択で完了払い戻し取引記録を第二のクライアントに送信する。
１８．第二のクライアントは任意選択で完了払い戻し取引記録が予想通りであり、第一の当事者および第二の当事者によって署名されたことを検証する。
１９．完了コミット取引と完了払い戻し取引の両方を作成または受信した後、第一のクライアントはソース取引を実行するための第一のソース取引記録を転送メカニズムに送信する。
２０．完了コミット取引と完了払い戻し取引の両方を作成または受信した後、第二のクライアントは第二のソース取引を実行するために第二のソース取引記録を転送メカニズムに提出する。
２１．第一のソース取引と第二のソース取引の両方が転送メカニズムに提出されたことを確認した後、第一のクライアントと第二のクライアントの一方または両方が、コミット取引を実行するための完了コミット取引記録を提出する。
２２．有効期限タイムスタンプ時もしくはその後、または条件によって定義される時点及び完了払い戻し取引記録のロックタイムの前に、ファシリテータは任意選択で一つ以上のデータソース（例えば、公的に取引された金融商品の最新の価格、オファーが受諾された時点での商品の価格など）を参考にし、第一の支払い額及び第二の支払額を決定するため

の条件を計算する。一実施形態では、データソースは、外部データフィード、内部データベース、他のデータソースなどを含む。
例示的な実施形態では、時間ｔが与えられると、データソースはｔ時点での基準資産、見積もり商品、基準資産としての名目資産b_t、資産q_tまたは基礎計量器の見積もり（例えば、基礎計器または見積もり計器が名目上の資産である場合）を行う。
上記の例に続くと、基本商品は米ドル、見積もりは豪ドル、資産はビットコインとなる。b_0は、取引が開始された時点のビットコインの米ドルの価値であり、b_fは、貿易が完了した時点のビットコインの米ドルの値である。q_0は貿易が開始された時点のビットコインの豪ドルの値であり、q_fは貿易が完了した時点のビットコインの豪ドルの値である。ファシリテータが第一の支払い額および第二の支払い額を計算するために使用する計算は、res_{base}（b_0，q_0、b_f、q_f）を含む。典型的な実施形態では、当事者
の損失は、相手方の利益に比例し、以下のことを暗示する。すなわち、以下のことを意味する：
【数２】

$$res_{quote}(b_0, q_0, b_f, q_f) = -res_{base}(b_0, q_0, b_f, q_f) \qquad [\text{eq. 2}]$$

２３．ファシリテータは、
（ａ）コミット取引からコミット額を受け取るための入力、
（ｂ）第一の支払い金額と第一の当事者の承認を必要とする第一の条件を含む第一の支払い出力、
（ｃ）第二の支払い額と、第二の当事者の承認を必要とする条件を含む第二の支払い額出力と、
（ｄ）第三者の承認を必要とする手数料および条件
を含む任意の第三の支払い出力を含む小切手取引記録に署名する。典型的には第一の支払い額、第二の支払い額および任意の手数料金額の合計は完了コミット取引のコミット額以下である。
支払い取引記録の例：

【表６】

```
Input:

      Previous tx: 6b24...b607

      Index: 0

      scriptSig: OP_0 [sig. placeholder] ddbb...b00601

Output:

      Value: 142500736

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 157479264

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 10000

      scriptPubKey: OP_DUP OP_HASH160 d377...5c8c OP_EQUALVERIFY
      OP_CHECKSIG

...
```

２４．ファシリテータは、第一クライアントと第二のクライアントの両方に未完了の取引記録を送信する。双方が相手側が完了払い戻し取引記録を提出する前に単独で支払い取引記録を転送メカニズムに検証、署名、提出することができる。

【００５２】

上記は、本発明による価値転送の一実施形態に過ぎず、他の実施形態では、同等または代替の手続きが利用されてもよい。以下は、非典型的であるが例示的な仕組みを含む実施形態を説明する。

１．第一クライアントは第二のクライアントにオファーを送信する。

２．第一クライアントはファシリテータにオファーを送信する。

３．ファシリテータは、完了コミット取引記録を作成するための未完了コミット取引記録を第一クライアントに送信する。未完了コミット取引記録には、

（ａ）第一ソース取引から第一元本金額を受け取るための第一元本の入力と、

（ｂ）（ｉ）第一の当事者、（ｉｉ）第二の当事者、（ｉｉｉ）ファシリテータの三者のうち二者の承認を必要とする条件の第一のコミット額を含む第一の入力、

が含まれる。

４．ファシリテータは、完了コミット取引記録を作成するための第二の未完了コミット取引記録を第二のクライアントに送信し、第二の未完了コミット取引記録は

（ａ）第二のソース取引から第二の元本金額を受け取るための第二の元本入力及び、

（ｂ）（ｉ）第一の当事者、（ｉｉ）第二の当事者、（ｉｉｉ）ファシリテータの三者の

うち二者の承認を必要とする条件の第二のコミット額を含む第一の入力が含まれる。
５．第一クライアントは第一ソース取引記録に署名する。
６．第一クライアントは未完了のコミット取引記録に署名する（例えば、ＳＩＧＨＡＳＨ＿ＳＩＮＧＬＥ　｜　ＳＩＧＨＡＳＨ＿ＡＮＹＯＮＥＣＡＮＰＡＹで）。
第一の未完了コミット取引記録の例
【表７】

```
Input:

      Previous tx: 85e5...e61f

      Index: 1

      scriptSig: 5e7c...a11a83 ecad...d0ba

...

Output:

      Value: 150000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

７．第一のクライアントは第一の未完了コミット取引記録をファシリテータに送信する。
８．第二のクライアントは第二のソース取引記録に署名する。
９．第二のクライアントは第二の未完了コミット取引記録を完了し、署名する（例えば、ＳＩＧＨＡＳＨ＿ＳＩＮＧＬＥ　｜　ＳＩＧＨＡＳＨ＿ＡＮＹＯＮＥＣＡＮＰＡＹで）。
第二の未完了コミット取引記録の例：

【表８】

```
...

Input:

      Previous tx: 705d...9ce2

      Index: 0

      scriptSig: ade1...9dcb83 f058...878a

...

Output:

      Value: 150000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

１０．第二のクライアントは第二の未完了コミット取引記録をファシリテータに送信する。

１１．ファシリテータは、第一の未完了取引記録と第二の未完了コミット取引記録から完了コミット取引記録を作成し、完了コミット取引記録は、

（ａ）第一ソース取引から第一元本金額を受け取るための第一元本入力と及び

（ｂ）第一コミット額と　（ｉ）　第一の当事者（ｉｉ）　第二の当事者（ｉｉｉ）ファシリテータのうち二者の承認を必要とする条件の第一のコミット額が含まれるコミット出力

（ｃ）第二のソース取引から第二の元本金額を受け取るための第二の元本入力及び

（ｄ）第二のコミット額及び（ｉ）第一の当事者（ｉｉ）第二の当事者（ｉｉｉ）ファシリテータのうち二者の承認を必要とする条件の第二のコミット出力

から構成される。

完了コミット取引記録例

【表９】

```
ID: 11f0...8ea8

Input:

      Previous tx: 85e5...e61f

      Index: 1

      scriptSig: 5e7c...a11a83 ecad...d0ba

Input:

      Previous tx: 705d...9ce2

      Index: 0

       scriptSig: ade1...9dcb83 f058...878a

  ...

  Output:

       Value: 150000000

       scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
       OP_CHECKMULTISIG

  Output:

       Value: 150000000

       scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
       OP_CHECKMULTISIG

  ...
```

別の実施形態では、ファシリテータが第一の未完了コミット取引記録や第二の未完了コミット取引記録を送信する前に第一のクライアントは第一のソース取引記録の取引ＩＤをファシリテータに提供し、第二のクライアントは第二のソース取引記録の取引ＩＤをファシリテータに提供する。ファシリテータは、第二の未完了コミット取引記録と同一の第一未完了コミット取引記録を作成し、各々は、プレースホルダシグネチャを有する第一の元本

入力と、プレースホルダシグネチャを有する第二の元本入力を含む。それぞれの未完了コミット取引記録がそれぞれのクライアントに送信されると、クライアントはそれぞれの署名された未完了コミット取引記録をファシリテータに返送する前に、それぞれの元本入力に（例えば、ＳＩＧＨＡＳＨ＿ＡＬＬ　｜　ＳＩＧＨＡＳＨ＿ＡＮＹＯＮＥＣＡＮＰＡＹで）署名する。ファシリテータは、署名された未完了のコミット取引記録を収集し、署名された入力を完了コミット取引記録に統合する。このような実施形態では、第一のコミット出力および第二のコミット出力を統合することができ、対応する支払い取引記録および払い戻し取引記録は、それぞれの第二の入力を省略することができる。

１２．ファシリテータは、完了したコミット取引記録を、任意選択で固定メモリに格納する第一のクライアントに送信する。

１３．ファシリテータは、完了したコミット取引記録を第二のクライアントに送信し、第二のクライアントは、選択的に固定メモリにそれを保存する。

１４．第一のクライアントは、以下を含む未完了の払い戻し取引記録に署名する（例えば、ＳＩＧＨＡＳＨ＿ＡＬＬ　｜　ＳＩＧＨＡＳＨ＿ＡＮＹＯＮＥＣＡＮＰＡＹ又はＳＩＧＨＡＳＨ＿ＳＩＮＧＬＥ　｜　ＳＩＧＨＡＳＨ＿ＡＮＹＯＮＥＣＡＮＰＡＹで）。

（ａ）有効期限タイムスタンプ後のロックタイム、

（ｂ）第一コミット取引からコミット額を受け取るための第一の入力、

（ｃ）第二コミット取引からコミット額を受け取るための第二の入力、

（ｄ）第一の払い戻し金額と第一の当事者の承認を必要とする第一の条件を含む第一の払い戻し出力、

（ｅ）第二払い戻し金額と第二当事者の承認を必要とする条件を含む第二払い戻し出力。

未完了払い戻し取引記録の例

【表１０】

```
Input:

      Previous tx: 11f0...8ea8

      Index: 0

      scriptSig: OP_0 78a2...203181 [sig. placeholder]

Input:

      Previous tx: 11f0...8ea8

      Index: 1

      scriptSig: OP_0 fdbe...893f81 [sig. placeholder]

...

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

１５．第一のクライアントは、未完了払い戻し取引記録及び完了払い戻し取引記録を第二のクライアントに送信する。

１６．第二のクライアントは未完了払い戻し取引記録から完了払い戻し取引記録を作成し（例えば、ＳＩＧＨＡＳＨ＿ＡＬＬ　｜　ＳＩＧＨＡＳＨ＿ＡＮＹＯＮＥＣＡＮＰＡＹ又はＳＩＧＨＡＳＨ＿ＳＩＮＧＬＥ　｜　ＳＩＧＨＡＳＨ＿ＡＮＹＯＮＥＣＡＮＰＡＹで署名する）固定メモリに保存する。

完了払い戻し取引記録の例

【表１１】

```
ID: eb09...3d15

Input:

      Previous tx: 11f0...8ea8

      Index: 0

      scriptSig: OP_0 78a2...203181 b765...fc4383

Input:

      Previous tx: 11f0...8ea8

      Index: 1

      scriptSig: OP_0 fdbe...893f81 91e4...4dd583

...

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

１７．第二のクライアントは、完了払い戻し取引記録を第一のクライアントに送信する。
１８．完了コミット取引記録と完了払い戻し取引記録の両方を作成または受信した後、第一のクライアントは、第一のソース取引記録を転送メカニズムに提出する。
１９．完了コミット取引記録と完了払い戻し取引記録の両方を作成または受信した後、第二のクライアントは、第二のソース取引記録を転送メカニズムに提出する。
２０．第一のソース取引記録と第二のソース取引記録の両方が提出されたことを確認した後、第一のクライアントと第二のクライアントの一方または両方が完了コミット取引記録を提出する。
２１．タイムスタンプの有効期限際またはその後、または条件によって決められた所定の時点で完了払い戻し取引記録のロックタイムの前に、ファシリテータは、第一と第二の支払い額を決定するための条件に従って計算を実行し、任意選択で、計算に使用するために一つ以上のデータソースから情報を要求する。
２２．ファシリテータは、未完了の支払い取引記録に署名する。（例えば、ＳＩＧＨＡＳ

Ｈ＿ＡＬＬ　｜　ＳＩＧＨＡＳＨ＿ＡＮＹＯＮＥＣＡＮＰＡＹ又はＳＩＧＨＡＳＨ＿ＳＩＮＧＬＥ　｜　ＳＩＧＨＡＳＨ＿ＡＮＹＯＮＥＣＡＮＰＡＹで）

未完了の支払い取引記録の例：

【表１２】

```
Input:

      Previous tx: 11f0...8ea8

      Index: 0

      scriptSig: OP_0 [sig. placeholder] 8cd3...d86481

Input:

      Previous tx: 11f0...8ea8

      Index: 1

      scriptSig: OP_0 [sig. placeholder] 12bc...825281

...

Output:

      Value: 142500736

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

 Output:

       Value: 157479264

       scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
       OP_CHECKSIG

 Output:

       Value: 10000

       scriptPubKey: OP_DUP OP_HASH160 d377...5c8c OP_EQUALVERIFY
       OP_CHECKSIG

  ...
```

２３．ファシリテータは、第一のクライアントと第二のクライアントの両方に未完了支払い取引記録を送信し、そのいずれかが先の例示的実施形態のようにそれを提出することができる。

【００５３】

簡潔にするために、様々な検証ステップが省略されている。

【００５４】

上記の各実施形態の態様が混合され得ることは、当業者には明らかになるであろう。例えば、第一のクライアントはファシリテータにオファーを送信することができ、第二の

クライアントはファシリテータを見つけてそれを引き出すことができる。上述したように、ファシリテータは当事者のどちらかまたは両方の代理人として行動することが求められているので、第一のクライアントおよび第二のクライアントの一方または両方の態様はファシリテータと一致することがあり、ファシリテータは余分とみなされた上記の手順の大部分を省略させることができる。ファシリテータは、片方のクライアントの態様を含むことができるが、もう片方の態様を含むことができない。その場合クライアントは任意選択で署名する前にファシリテータから受信した取引記録を　独立に検証することができる。そのような実施形態では、ファシリテータは典型的にウェブベースのユーザインターフェース（ＵＩ）、アプリケーションプログラマインターフェース（ＡＰＩ）などのインターフェースを介してクライアントの態様を制御する方法を含む。

【００５５】

このような実施形態では、ファシリテータに権限を委任する当事者は、ファシリテータが安全で公正に行動することを信頼しなければならないが、これは多くの当事者が従来の第三者仲介者に対して既に有する期待と同様である。　第一の当事者はファシリテータが第一の当事者の代理として働くために同じキーペアに独立したアクセスを持ち、同様に第二の当事者はファシリテータが第二の当事者のために行動するための同じキーペアに独立したアクセスを持つので、もしファシリテータが破棄されても、最悪の場合でも完了払い戻し取引記録のコピーを固定メモリに保存していれば、第一当事者と第二当事者は、ロックタイム以降に完了払い戻し取引記録を提出することで彼らの資産を取り戻すことができる。

【００５６】

一実施形態ではクライアントは新しい消費可能な出力を検出した場合（例えば、ビットコインまたは類似の転送メカニズムを持つプロトコルを使用する場合にブロックチェーンの変更または更新を監視することによって）、自動的に新しい消費可能な出力と同程度の遠隔オファーを受け入れる。また別の実施形態ではクライアントが第二の使用可能な出力を検知した場合、それを無効にしようとする。成功すれば、新しい消費可能な出力の一部及び全部を含めた新しいオファーを発信する。他のバリエーションも可能である。例えば、クライアントは利用可能なオファーをスキャンし、消費可能な出力と一致するように設定することもできる。アルゴリズムは当技術分野では知られており、複雑性はそれぞれ異なる。例えば、ビットコインプロトコルのクライアント実装は簡単な取引の入力と消費可能な出力が一致するようなアルゴリズムを提供している。そのようなアルゴリズムは一般的な技術を持った当業者や類似した発明の実施形態によって適応可能である。

【００５７】

複数の実施形態においてこれらの条件は任意選択で第一の証券と第二の証券が資産に指定される比率、および各参加者が割り当てなければいけない金額を含む。例えば一実施形態では、これらの条件は、各当事者から３　ビットコインの所要配分で２ビットコイン／米ドルを「売却」することを提供することができ、換言すれば、２ビットコインの米ドルに対するエクスポージャーを提供し、参加者は、スワップの期間（すなわち、期限が切れるまで、または一方の当事者の元本および担保が使い尽くされるまで）、ビットコインを元本２枚とビットコイン１枚を担保に配分する必要がある。

【００５８】

各当事者の割り当ては同等である必要はない。ある実施形態で市場がある特定の商品ペアがスワップの継続期間に低下すると予想している場合はその商品ペアへのエクスポージャーを受諾する当事者が相手より多くの担保を割り当てられることが求められる場合もある。前述の例では当事者間のリスクは非対称である。オファー側が損失する最大の額は２ビットコイン（ビットコインが米ドルで無価値になる場合）である。しかし、受け取る側の損失は際限がない（ビットコインに対して米ドルが無価値になる場合）、従って、

【数３】

$$res_{base}(b_0, q_0, b_f, q_f) = principal \times \frac{b_f - b_0}{q_f - q_0} \quad [\text{eq. 3}]$$

【００５９】

代替案は：

【数４】

$$res_{base}(b_0, q_0, b_f, q_f) = principal \times \left(\frac{b_f}{q_f} - \frac{b_0}{q_0} \right) \quad [\text{eq. 4}]$$

【００６０】

他の実施形態では対称的なモデルを採用することができる。

【数５】

$$res_{base}(b_0, q_0, b_f, q_f) = \begin{cases} \frac{b_t}{q_f} \leq \frac{b_0}{q_0} & : principal \times \left(\frac{b_f q_0}{b_0 q_f} - 1 \right) \\ \frac{b_t}{q_f} > \frac{b_0}{q_0} & : principal \times \left(1 - \frac{b_0 q_f}{b_f q_0} \right) \end{cases} \quad [\text{eq. 5}]$$

【００６１】

ここで、ｒｅｓ$_{base}$（…）は、当時のベース証券の初期値ｂ$_0$、見積り証券の初期値ｑ$_0$、ｆ時点のベース証券の価値ｂ$_f$、ｆ時点の見積り証券の価値ｑ$_f$が条件のベース証券のエクスポージャーを取った当事者の損益である。見積もり証券のエクスポージャーを取っている当事者の結果的な損益は逆転する。

【数６】

$$res_{quote}(b_0, q_0, b_f, q_f) = -res_{base}(b_0, q_0, b_f, q_f)$$

$$= \begin{cases} \frac{b_f}{q_f} \leq \frac{b_0}{q_0} & : principal \times \left(1 - \frac{b_f q_0}{b_0 q_f} \right) \\ \frac{b_f}{q_f} > \frac{b_0}{q_0} & : principal \times \left(\frac{b_0 q_f}{b_f q_0} - 1 \right) \end{cases} \quad [\text{eq. 6}]$$

【００６２】

この実施例では、当事者のリスク式は対称である。ベース証券がゼロになる場合でも、ベース証券エクスポージャーを持つ当事者が失うのは元本のみである。同様に見積もり証券がゼロになった場合、見積もり証券のエクスポージャーを持つ当事者が失うのは元本のみである。担保が不要であることに留意されたい。代替案として、以下が考えられる。

【数７】

$$res_{base}(b_0, q_0, b_f, q_f) = -res_{quote}(b_0, q_0, b_f, q_f)$$

$$= \begin{cases} \frac{b_f}{q_f} \leq \frac{b_0}{q_0} & : -principal \times \frac{b_0 q_f}{b_f q_0} \\ \frac{b_f}{q_f} > \frac{b_0}{q_0} & : principal \times \frac{b_f q_0}{b_0 q_f} \end{cases} \quad [\text{eq. 7}]$$

【００６３】

この実施例では当事者のリスク計算式も対称である。しかし基本資産がゼロになれば基本資産をとった当事者の損失は無限に近づき他の全ては同等になる。同様に、見積もり資産がゼロになれば、見積もり資産を取った当事者が被った損失も無限大に近づき、他の全ては同等になる。損失が元本金額を超えた場合に担保が必要であることに留意されたい。

より変動性の高い商品ペアは、有効期限する前に終了してしまう危険性を最小限にするためにより多くの担保が必要とされうる。これらは基本的な例である。割り当て支払額を決定するための計算に影響を与える条件は、任意に複雑にすることができ、参加者の想像力によってのみ制限されている。全てのそのような変形は本発明によって企図されている。

【００６４】

当事者の片方が期限が切れる前に価値の転送（例：スワップ）を終了したいと望む状況もある。当事者の双方が途中で終了することに同意することもある。一実施形態では、ファシリテータは当事者が終了することに合意したときに、スワップの期限が切れたかのように未完了の支払い取引記録を作成することによってこれを容易にする。終了を要求する側の当事者は、未完了の支払い取引記録に署名し合意する側の当事者へ送信し、合意する側の当事者は転送メカニズムにそれを提出する。ファシリテータは第三者への手数料の出力が含まれている場合、合意する側の当事者は手数料が要求する側の当事者によって多くもしくは全額負担されることを要求することがある。

【００６５】

当事者の片方が期限が切れる前に価値の転送を終了したいと望んでいるが相手側の合意をとりつけられない場合、終了したい側が第三者の代理を探すことが別の選択肢の一つである。図６及び図７はそのような代理が含まれるスワップ実施形態の様々な例を示している。

【００６６】

図６は撤退する側（Ａ）が参入者（Ｃ）がＡに代わって残存する側（Ｂ）と価値転送をするように納得させた場合である。更に、参入者は撤退側に交渉した額（ε）を支払う。これはこの実施形態の中で、代理取引、第二コミット取引、第二払い戻し取引によって円滑化される。

【００６７】

明確に説明するために、コミット取引の出力と対応する代理取引の入力は第一の元本（P_A）第一の担保（C_A）第二の元本（P_B）第二の担保（C_B）と分けて示されている。これは本発明の制限ではない。前述の実施形態のように、コミット取引の出力とそれに対応する代理取引の入力は転送メカニズムによって有効とみなされたどのような構造でも良い。代理取引の出力と第二コミット取引の入力は明確に説明するために同様に描かれている。また、取引間での入力と出力の全ての構造は本発明で予期されている。

【００６８】

差分（δ）は取引が代理された時点で期限が切れたと仮定して第一支払い額と第二支払い額を計算するための差である。図６に示された実施形態のようにこれは残留する側に有利である。代理取引記録は撤退側がその差額のロスを受け入れ、参入側が空いたポジションを埋めるための資産を供給する構造になっている。

【００６９】

また図６に示される実施形態では代理払い戻しは非対称である。参入側はその当事者がコミットした取引（から交渉した分を引いたもの）を払い戻しされ、残留する側は代理時にスワップが有効期限になったと仮定した受け取り分を払い戻しされる。他のバリエーションも可能である。例えば、実施形態の一つでは交渉された額が価値転送の他の段階や全く他の価値転送で分けて転送されることも可能である。

【００７０】

図７に示される実施形態では、代理は撤退側に有利である。その実施形態では代理払い戻しは対称である。残留側はもともとの取引が払い戻しされる分を受け取る。

【００７１】

ある実施形態では代理は次のように円滑化される。

１．ファシリテータは撤退額を決定するための条件に沿って計算を実行し、任意選択でその計算のために一つ以上のデータソースからの情報を要求する。

２．ファシリテータは、

（ａ）コミット取引から金額を受け取るための第一入力、

（ｂ）ソース取引からエントリ金額を受け取るためのエントリ入力、
（ｃ）撤退金額と第一の当事者の承認が必要な条件を含む撤退出力、
（ｄ）代理金額と（ｉ）第二当事者（ｉｉ）第三当事者（ｉｉｉ）ファシリテータのうちの二人からの承認が必要な第二の条件を含んだ代理出力、
を含む未完了の代理取引記録を作成する。
未完了の代理取引記録の例：
【表１３】

```
Input:

      Previous tx: 6b24...b607

      Index: 0


        scriptSig: OP_0 [sig. placeholder] [sig. placeholder]

  Input:

      Previous tx: dd66...ae8e

      Index: 3

      scriptSig: [sig. placeholder]

  Output:

      Value: 300000000

      scriptPubKey: 2 bf9a...f9e3 952b...0542 cffd...1373 3
      OP_CHECKMULTISIG

  Output:

      Value: 121871000

      scriptPubKey: OP_DUP OP_HASH160 6250...6cfc OP_EQUALVERIFY
      OP_CHECKSIG

  ...
```

３．ファシリテータは、第一当事者と第三当事者に未完了の代理取引記録を送信する。
４．第一当事者は第一の未完了の代理取引記録に署名することによって署名された未完成代理取引記録を作成し（例えば、ＳＩＧＨＡＳＨ＿ＡＬＬ　｜　ＳＩＧＨＡＳＨ＿ＡＮＹＯＮＥＣＡＮＰＡＹによって署名して）、ファシリテータへ第一の未完了の代理取引記録を送信する。
５．第三当事者は　未完了の代理取引記録に署名することによって（例えば、ＳＩＧＨＡＳＨ＿ＡＬＬ　｜　ＳＩＧＨＡＳＨ＿ＡＮＹＯＮＥＣＡＮＰＡＹによって署名して）、第二の未完了の代理取引記録を作成し、第二の署名された代理取引記録をファシリテータに送信する。
６．ファシリテータは完了した代理取引記録（例えば、ＩＤ：９ｃ８ｂ．．．４７９４）を第一と第二の未完了の代理取引記録を使って作成する。

７．ファシリテータは、
（ａ）有効期限タイムスタンプ後のロックタイム、
（ｂ）代理取引から代理金額を受け取るための入力、
（ｃ）第一の払い戻し金額と第二の当事者の承認が必要な条件が含まれる第一の払い戻し出力及び、
（ｄ）第二の払い戻し金額と第三の当事者の承認が必要な条件が含まれる第二の払い戻し出力、
を含む未完了の代理払い戻し取引記録に署名する。
未完了の代理払い戻し取引記録の例：
【表１４】

```
Input:

      Previous tx: 9c8b...4794

      Index: 0

      scriptSig: OP_0 [sig. placeholder] b2ac...8a4601

Output:

      Value: 178124000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 121866000

      scriptPubKey: OP_DUP OP_HASH160 94e2...4fb6 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

８．ファシリテータは、未処理の代理払い戻し取引記録に署名して署名付きの代理払い戻し取引記録を作成し、署名付きの代理払い戻し取引記録を第二の当事者及び第三の当事者に送信する。
９．ファシリテータは、完全な代用還付取引記録を転送メカニズムに提出する。
【００７２】
前述の実施形態に含まれる様々な検証や手順の詳細は簡潔さのために省略されている。他の実施形態では様々な取引記録がファシリテータではなく第一の当事者や第二の当事者によって作成または署名されている。例えば、第一の当事者や第二の当事者は代理の取引記録の金額に同意する可能性があり、ファシリテータを必要とせずに署名することができる。全てのそのようなバリエーションは想定されている。
【００７３】
信用状（Ｌ／Ｃ）は当分野ではよく知られているが、それは根本的には第三者が事前に合意された条件が果たされている場合に所定の時点以前に第一の当事者の代理として第二の当事者に価値を転送するという合意である。典型的には買い手の資金を解放する前に高額な仲介金融業者による手動での難解な出荷書類の見直しなどが含まれる。しかしこのような高額なアプローチはファシリテータが支払い取引記録を出荷者の公開ＡＰＩなどの既知のトラッキングナンバーや他の実施形態、信用状（Ｌ／Ｃ）の評価調査結果、予想され

る場所でのデータの有無の観察、ＡＰＩからの変数または応答の値が一連の期待値内にあるか、または予想されるパターンに一致するかどうかのチェック、デジタル機器から信号を受信するか（温度センサ、ＧＰＳなど）そして信号値が予想される範囲または許容値内であることを検証するステップなどの質問の結果に基づいた支払い取引の発信や作成を条件づける本発明の一実施形態により回避されることができる。例えば、米国特許出願第１３／９７０，７５５号（'７５５）は、地理空間的な近さを効率的に計算するためのシステムおよび方法を記載している。他のものは当該技術分野で知られている。一実施形態での計算は物体が特定の位置の「ａｔ」または「ｎｅａｒ」（すなわち、特定の距離以内）であった状態を含む。（例えば、既知の場所にある報告検出器またはセンサの近傍の自己報告ＧＰＳ、バーコード、クイックレスポンス（ＱＲ）コード、無線周波数識別（ＲＦＩＤ）タグなどの自動識別およびデータキャプチャ（ＡＩＤＣ）装置など ）に送信することができる。多くの可能な構造が本発明によって想定されており、当業者には明らかになるであろう。

【００７４】

図８はソース取引およびコミット取引を備えた信用状（Ｌ／Ｃ）に関連する一実施形態の態様を示している。図示のようにコミット取引は第一の金額を第一のソース取引（例：第一の当事者）から受け入れるための第一の入力、または第一の金額を一つ以上の取引に注入するための出力（図示なし）を含んでいる。他の実施形態での（他の図に示されている）コミット取引は、第二のソース取引から第二の金額を受け入れるための第二の入力を含む。ここで第一の金額と第二の金額の合計は様々な図に示されているようにいくつかのケースでは元本額（Ｐ）、および（任意選択で）担保額（Ｃ）を含む。第一のソース取引のみ図８に示されているが。本発明の限定として解釈されるべきではない。

【００７５】

図９はコミット取引、前述の実施形態に示された払い戻し取引と同義の有効期限取引、信用状に関連する一実施形態の態様を示している。ただし、払い戻し取引は例外が発生した場合の資金の回収のために排他的な意味を持つことに加え（ファシリテータが支払い記録を作成または署名できなくなる場合など）、資金回収に加え有効期限取引の使用は オファー（ファシリテータが参加していたのに設定された条件が期限タイムスタンプ内に満たされていないなど）により想定される。違いは大部分が概念的である。本発明の範囲内では二つはほとんど同じ機能である。コミット取引は第一の元本（P_A）およびコミット出力を受信するための第一の入力を含んでいる。有効期限取引は第一の当事者への第一の出力であるコミット出力の金額を受信するための入力を含み、第二の金額を受信するための第二の入力を含む他の実施形態では第二当事者のための第二出力を含む。

【００７６】

図１０－１１は、元本と担保が関わる状況での信用状を含む比較的単純な支払い取引を含む実施形態の態様を示す。図１０は第一当事者からの元本および担保（（Ｐ＋Ｃ）$_A$）の入力を含んでいる。他の実施形態では、ちょうど上述したものと同様に入力は結合される必要はない。図１１のコミット取引が第一のとうじしゃからの最初に加えた元本および担保入力、そして第二当事者からの第二担保（C_B）の入力を含んでいる。これらは、本発明によって企図される多くの可能な構成のうちの二つである。たとえば、コミット取引は、第一の相手からの主要な入力を含むことができる第三者から担保の入力（例えば、図示していない第一当時者からの保証など）および第二者から担保入力などから構成される可能性もある。

【００７７】

図１０－１１に示される実施形態では、支払い取引の各コミットの出力の金額を受け取るための入力を含む。図１０は、支払い取引は、第一の当事者への第一の担保支払い出力、第二者への第一の元本出力、および担保から控除される任意の手数料の出力を備えている。図１１、支払いの取引は第一の当事者への担保支払いの出力を備えており、参加元本および担保貸付実行、第二当事者に出力される。また、コミット取引は支払い取引における当事者が均等に負担する第三者へのオプション料の出力を備える。これらは本発明の多

くの可能な構成の二例でしかない。例えば、任意の手数料の出力はどの段階、及びどの複数の段階でも割り当てられることができる。また当事者の一人によって偏って負担されることもできる。

【００７８】

上記の様々な構成要素がどのように信用状の合意を円滑化するために使用できるかを例示的に示すため、転送メカニズムとしてビットコインまたは類似のプロトコルを使用している次の手順は一実施形態で起こるものである。この実施形態では、当事者は互いを信頼しておらず、ファシリテータもどちらの当事者にも完全には信頼されていない：

１．第一のクライアントが、

（ａ）データソースへの１つ以上の参照を含む支払い条件、データソースへの１つまたは複数の参照を含む支払い機能、およびデータソースへの１つ以上の参照を含む支払い条件、

（ｂ）元本金額、

（ｃ）期限タイムスタンプ、

（ｄ）任意の第一の担保金額、

（ｅ）任意の第二の担保金額、

を含む条件を含むオファーを作成する。

条件例：

【表１５】

```
Payer principal: 0.5 (BTC)

Payer collateral: 1 × principal

Payee collateral: 0.05 × principal

  Disbursement condition:

  FedEx("987654321").deliveredToCarrier() == true

  Expiration: 2014-06-01T12:34:56Z

  ...
```

２．第一のクライアントは、第一のソース取引記録に署名する。

３．（ａ）第一のソース取引から第一の金額を受け取るための第一の入力と、

（ｂ）任意選択で第二のソース取引から第二の金額を受け取るための第二の入力と、

（ｃ）コミット金額と（ｉ）第一の当事者（ｉｉ）第二の当事者（ｉｉｉ）第三の当事者のうち二人の承認が必要な条件を含むコミット出力、

が含まれる第一の未完了のコミット取引記録を作成する。

４．第一のクライアントは任意選択でオファーをファシリテータに送信し、ファシリテータはオファーを検証する。（有効期限のタイムスタンプが許容範囲内であることや、条件を解釈することができることなど）検証が失敗した場合、ファシリテータは、必要に応じてオファーを拒否することができ、任意選択でエラーメッセージをクライアントに送信することができる。

５．第一のクライアントは、第二のクライアントにオファーを送信する。

６．第二のクライアントはソース取引記録を作成する。第二のクライアントは未完了のコミット取引記録を第一のクライアントに送信する。

７．第一のクライアントは未完了のコミット取引記録に署名する（例えば、ＳＩＧＨＡＳ

Ｈ＿ＡＬＬ　｜　ＳＩＧＨＡＳＨ＿ＡＮＹＯＮＥＣＡＮＰＡＹで）ことによって完成したコミット取引記録を作成し、任意選択で完全なコミット取引記録を固定のメモリに保管する。

完全なコミット取引記録の例：

【表１６】

```
ID: c215...fc9b

Input:

      Previous tx: 85f7...e06c

      Index: 4

      scriptSig: 186b...ed3d81 9a9c...0fc5

Input:

      Previous tx: 6b03...e16e

      Index: 7

      scriptSig: c48e...353c81 4afe...2c8d

...

Output:

      Value: 150000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

８．第一のクライアントは、次のものを含む未処理有効期限取引記録に署名する。

（ａ）有効期限のタイムスタンプ以降のロックタイム、

（ｂ）コミット取引からのコミット金額を受け取るための入力、

（ｃ）第一の有効期限額と第一の当事者の承認を必要とする条件からなる第一の有効期限出力、

（ｄ）任意選択として、第二の有効期限額と第二の当事者の承認を必要とする条件からなる第二の有効期限出力。

完了有効期限取引記録の例：

【表１７】

```
Input:

      Previous tx: c215...fc9b

      Index: 0

      scriptSig: OP_0 7d17...0b5101 [sig. placeholder]

...

Output:

      Value: 99995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 4995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-01T12:34:56Z
```

９．第一のクライアントは、完了コミット取引と未完了有効期限取引記録を第二のクライアントへ送信し、第二クライアントはそれを任意選択で固定メモリに保管する。
１０．第二のクライアントは未完了有効期限取引記録に署名することで完了有効期限取引記録を作成し、完了有効期限取引記録を任意選択で固定メモリに保管する。
１１．第二のクライアントは第一のクライアントに完了した有効期限取引記録を送信する。
１２．完了有効期限取引記録及び完了コミット取引記録を作成もしくは受け取った後、第一のクライアントは第一のソース取引を行うために、転送メカニズムに第一のソース取引記録を提出する。
１３．第二のクライアントは完了有効期限取引記録及び完了コミット取引記録を作成もしくは受け取った後、第二のソース取引を行うために、転送メカニズムに第二のソース取引記録を提出する。
１４．第一のソース取引記録と第二のソース取引記録の両方が提出されたことを確認したのち、第一または第二のクライアントの一方または両方は、完全なコミットトラ取引記録を転送メカニズムに送り、コミット取引を実行する。
１５．条件により定義された時点もしくは第一及び第二のクライアントからの問い合わせ（任意選択で完全コミット取引記録、コミット取引への参照、および条件のうち
の一つ以上を提供する）により、有効期限取引記録の完全なロックタイムの前にファシリテータは第一の支払額、任意選択で第二の支払額の計算を実行し、任意選択で計算に使うための情報をデータソースに要求することもある。（例えば予定された出荷が荷送人に送付されたかどうかなど）これは外部のＡＰＩや内部データベースの照会などで可能である

。
典型的な実施形態では、支払い金額は残っている担保がそれぞれの提供側に戻され、元本が提供側（支払人）から取引先（受取人）に移転するようなものである。
１６．ファシリテータは、
（ａ）コミット取引からコミット額を受け取るための入力と、
（ｂ）第一の支払い額と、第二の当事者の承認を必要とする第一の条件とを含む第一の支払い出力と、
（ｃ）第二の支払い額と、第一の当事者の承認を必要とする条件を含む第二の支払額出力と、
（ｄ）第三者の承認を必要とする条件とを含む第三の支払い出力と、
であって、典型的には、第一の支払い額、第二の支払い額、および任意の料金額の合計がコミットからコミット額を超えないものを含む、未完了の取引または取引記録に署名する。
未完了支払い取引記録の例：
【表１８】

```
Input:

      Previous tx: c215...fc9b

      Index: 0

      scriptSig: OP_0 [sig. placeholder] 8205...424901

Output:

      Value: 49990000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 54990000

      scriptPubKey: OP_DUP OP_HASH160 6250...6cfc OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 10000

      scriptPubKey: OP_DUP OP_HASH160 d377...5c8c OP_EQUALVERIFY
      OP_CHECKSIG

...
```

１７．前述の実施例のように、ファシリテータは転送メカニズムにそれに署名し、いずれも提出することができる第一のクライアントと第二のクライアントの両方に未完了支払い取引記録を送信する。
【００７９】

別の実施形態では、コミット出力の状態が第一当事者と第二当事者または第二当事者と一人以上のサービスプロバイダ（例えば荷主、保険会社、検察官など）のいずれかの承認が必要である。未完了支払い取引記録は、第二当事者のプレースホルダ、およびサービスプロバイダによって構成されている。サービスプロバイダ全員がそれぞれ署名した場合、第二者が署名し転送メカニズムに支払い取引記録を提出することができる。さらに他の実施形態では、第二の当事者がコミット取引にサービスプロバイダへ支払いをするためのコミット取引に資産をコミットした場合はサービスプロバイダは各自支払い取引から支払われている。

【００８０】

図１２から図１４は　当事者の置換を含む様々な一連の信用状の実施形態例を示す。図１２は、支払人（Ａ）が受取人（Ｂ）との取引に代入するように代入者（Ｃ）を納得させた実施形態の態様を示している。また、支払人は代入者に交渉された量（ε）を転送する。例えば、支払人の当事者が受取人から商品を購入することを約束している場合、予期せぬ市場状況のために代入者に商品を受け取る権利を売却することを損失を見込んで決めた。これは示された実施形態において代理取引と第二有効期限取引によって円滑化される。関連の実施形態では支払人が利益の配分を受け取る権利を売却し、交渉された金額は、代入者から支払人へ渡される可能性がある。図１２に示す実施形態では。任意の手数料（φ）が第三者に支払われ、それは受取人によって負担されている。

【００８１】

図１３は、受取人（Ｂ）は、支払人（Ａ）との取引に代入する代入者（Ｃ）を納得させた実施形態の態様を示している。また、代入者は支払人に交渉された量（ε）を転送する。例えば、第三者はおそらく代入者の他の資産の減少相対値に将来の支払い取引で支払を受ける権利を持つことに興味がある可能性がある。これは示される実施形態では代理取引によって円滑化され、受取人が支払いを受ける権利を売却した関連の実施形態では交渉された金額が代入者に支払われる可能性もある。図１２と同様に図１３では任意の手数料（φ）が第三者に支払われ、それは代入者によって負担されている。

【００８２】

図１４は、支払人（Ａ）が代入者（Ｃ）が（当初は支払人によって支払われた担保をカバーするように示されているように）受取人（Ｂ）との取引を部分的に代入するようにした態様を示す。さらに、代入者は交渉された金額（ε）を支払人に転送する。これは、図示された実施形態では、代理取引および第二有効期限取引によって円滑化され、いくつかの実施形態では、代理取引の代理出力は、三者のうちの三者、四者のうちの三者、四者のうちの二者などの承認が必要な条件をふくむ（例えば、代入者が代理権を委任され支払人に代わって承認または署名する権限が与えられている場合）。多くの可能な構成が本発明によって企図される。そのような実施形態では、ファシリテータは、以下に説明するように選択された仲介者との取引に異議を唱える能力を維持するなど、すべての当事者が満足する代理取引を作成する際に審判員として行動することができる。

【００８３】

図中の説明を明確にするために図１２から図１４はコミット取引の出力やそれに対応する代理取引の入力は元本および担保（$(P+C)_A$）と及び第二の担保（C_B）として個別に示されている。これは本発明の制限ではない。コミット取引の出力やそれに対応する代理取引の入力は転送メカニズムによって有効とみなされたどのような設定でもよい。代理取引の出力および第二コミット取引への入力は説明目的のために示されている。入力や出力の全ての有効な設定はこの発明により企図されている。更に別の実施形態ではいかなる手数料においてもどの当事者（第四者でもよい）が一部もしくは全部を払って良い。

【００８４】

（例えばビットコインプロトコル、Ｅｔｈｅｒｅｕｍプロトコルなどの）転送メカニズムとして使用される分散型デジタル通貨では、本発明の別の実施形態は、任意のスワップ、信用状　など、ファシリテータによってそれを示す条件が表現または理解されるオファーならどのような任意のオファーも、その条件や条件の参照（ＵＲＬや条件のハッシュな

ど）、組み合わせなどが、取引メカニズム外の（分散型デジタル通過では「オフブロックチェーン」と呼ばれる）中央権威や共有分散データストア（トレントやアルトコインなど）ではなく取引記録自体にエンコードされていれば、特別取引記録を提出することにより可能である。

【００８５】

一実施形態では、これは取引記録メタデータ及び入力または出力（例えば、＜ｄａｔａ＞　ＯＰ＿ＤＲＯＰ　＜ｓｃｒｉｐｔ＞、ＯＰ＿ＲＥＴＵＲＮ　＜ｄａｔａ＞テクニックを介した単一出力など）の未使用データとして符号化することができる。説明のために、以下のステップではそのような多様な実施形態のうちの数例を記載する：

１．一実施形態では、第一のクライアント（提供者）は、関連データを含むオファー取引記録と、任意選択で第一当事者およびファシリテータのうちの一人の承認を必要とするオファー額および条件を含むオファー出力を作成する。関連データは、条件の一つまたは両方と条件に対する参照を含む。任意選択で関連データは、ファシリテータへの参照（例えば、ドメイン名、支払いアドレス、Ｄ＆Ｂ番号、ＵＲＩなど）を含む。任意選択で第一のクライアントは転送メカニズムにそれを提出する前に、条件、関連データ、オファー取引記録を検証のために（例えば、ファシリテータが用語を解釈することができ、ファシリテータが適切に特定されていることを確実にするために）ファシリテータに送信する。別の実施形態では、第一のクライアントの要求で、ファシリテータは完了オファー取引記録を作成するための第一の未完了オファー取引記録（署名された入力を含まないなど）を作成し、第一のクライアントは任意選択でファシリテータ提供のリファレンス（該当する場合）などで利用可能かどうか、ファシリテータは正確に未完了オファー取引記録を作成したかなどを検証する。

未完了オファー取引記録の例：

【表１９】

```
% # Post the terms to the facilitator
% curl -X POST -d
'{"base":"USD","quote":"AUD","denom":"BTC","pcpl":0.5,"cltl":1.0,"res":
"symunbound","offerexp":"2014-06-01T00:00:00Z","swapexp":"2014-07-
01T00:00:00Z","facuri":"https://facilitator.dom/api/v1"}' ...
https://facilitator.dom/api/v1/swap
{"ok":true,"offersha256":"3a72...f9a4","offerref":"facswap:3a72...f9a4"
,"offeruri":"https://facilitator.dom/api/v1/swap/3a72...f9a4"}

      ID: 9fcd...429c

      ...

      Output:

            Value: 150000000

            scriptPubKey: 666163737761703a3a72...f9a4 OP_DROP 1
            67c1...4a70 cffd...1373 2 OP_CHECKMULTISIG

      ...
```

この例示的な実施形態では、ファシリテータは、条件のハッシュの最初に「６６６１６３７３７７６１７０３ａ」をつけ、それは８バイトのＡＳＣＩＩ文字列「ｆａｃｓｗａｐ：」の１６進数である。これは必ずしも必要ではないが、取引が特定の「タイプ」であると

認識される便利な手段であり、ネットワーク参加者による監視に役立つ。
別の実施形態のオファー取引記録の例：
【表２０】

```
% # Post the terms to the facilitator
% curl -X POST -d '{"pubkey":"67c1...4a70","terms":
{"base":"USD",...,"facuri":"https://facilitator.dom/api/v1"}}' ...
https://facilitator.dom/api/v1/swap
{"ok":true,"offersha256":"3a72...f9a4","offerref":"facswap:3a72...f9a4"
,"offeruri":"https://facilitator.dom/api/v1/swap/3a72...f9a4","offertxn
":"04000000...0280d1f008000000008901014b67c1...4a704bcffd...13730102ae.
..0000000000000002a6a2866163737761703a3a72...f9a400000000"}
% # Validate "offertxn", add change outputs, etc.
```

"offertxn" is annotated as follows:

```
04000000 [version: 4] ... 02 [output count: 1] 80d1f00800000000
[amount: 1.5 BTC] 89 [script len: 137] 01 [push next 1 byte] 01 [1] 4b
[push next 75 bytes] 67c1...4a70 [pub. key] 4b [push next 75 bytes]
cffd...1373 [fac. pub. key] 01 [push next 1 byte] 02 [2] ae
[OP_CHECKMULTISIG] ... 0000000000000000 [amount: 0.0 BTC] 2a [script
len: 42] 6a [OP_RETURN] 28 [push next 40 bytes]
666163737761703a3a72...f9a4 [offerref: "facswap:3a72...f9a4"] 00000000
[lock time: none]
```

いくつかの部分（入力やプレースホルダなど）には読みやすさを助けるために省略記号を省略していることに留意されたい。別の実施形態では親取引に通常存在するであろう出力スクリプトを隠すためにＰａｙ－ｔｏ－Ｓｃｒｉｐｔ　Ｈａｓｈ（Ｐ２ＳＨ）が使用されている。このような実施形態では、実際の出力スクリプトは、他の何らかの手段を介して必要な参加者に送信される。

２．ある実施形態では、第一のクライアントが未完了のコミット取引記録を作成し、もう一つの実施形態ではファシリテータが完了コミット取引記録を作成しており、第一のコミット入力がオファー取引からオファー額を受けとるためのものであり、第二の入力がまだ見つかっていないソース取引から金額を受け取るためのであるものを除いた前述の実施形態のようである。
３．第一のクライアントは、未完了オファー取引記録に署名することによって完了オファー取引記録を作成し、　オファー取引を実行するためにそれを転送メカニズムに提出する。
４．ファシリテータは転送メカニズムからオファー取引を受信する。
５．第二のクライアントは、ファシリテータにパブリックキーを送信する。
６．ファシリテータは、パブリックキーを未完了コミット取引記録に追加し、第一コミット取引記録を第二のクライアントに送信する。
７．第二のクライアントは取引ＩＤを有するソース取引記録に署名する。
８．第二のクライアントは、取引ＩＤを未完了コミット取引記録に追加して署名する。
未完了コミット記録取引記録の例：

【表２１】

```
Input:

      Previous tx: 9fcd...429c

      Index: 0

      scriptSig: [sig. placeholder]

Input:

      Previous tx: b5e8...6f57

      Index: 6

      scriptSig: 9b6b...8f3701 ac2f...b01b

...

Output:

      Value: 149990000

      scriptPubKey: 2 67c1...4a70 dbe4...4cbe cffd...1373 3
      OP_CHECKMULTISIG

...
```

９．第二のクライアントは、署名された未完了コミット取引記録をファシリテータに送信する。
１０．第一のクライアント及び任意選択で（許可されている場合）ファシリテータは　未完了のコミット取引記録に署名することによって完了コミット取引記録（ＩＤ：６９９６．．．　ｅｃ３ｄなど）を作成し、任意選択で固定メモリに完了取引記録を保管する。
１１．ファシリテータは、未完了の払い戻しや有効期限取引記録を作成し、未完了の払い戻しや有効期限取引記録を第二のクライアントに送信する。
１２．第二のクライアントは、未完了の払い戻しまたは有効期限取引記録に署名し、署名された未完了の払い戻しまたは有効期限取引記録をファシリテータに送信する。
１３．第一クライアント及び任意選択で（許可されている場合）ファシリテータは、払い戻し取引記録に署名することにより完了払い戻しまたは有効期限取引記録を作成し、完了払い戻し取引または完了有効期限取引記録を固定メモリに格納する。
１４．ファシリテータは、完了コミット取引記録を送信し、完了払い戻しまたは完了有効期限取引記録を第二のクライアントに送信する。
１５．第二のクライアントは、ソース取引を実行するためにソース取引記録を転送メカニズムに提出する。
１６．ソース取引が提出されたことを確認した後、第一のクライアント、第二のクライアント、およびファシリテータのうちの一人、数人、または全員は、完了コミット取引記録を転送メカニズムに提出し、その後のプロセスは前述の実施形態と類似している。

【００８６】

別の実施形態では、オファーは「ハードオファー」を含み、オファー出力の条件は第一当事者およびファシリテータの両方の承認を必要とし、ファシリテータはある時点に設定されたロックタイムと、前記オファー額を受け取る入力と、第一当事者の承認を必要とす

る有効期限および条件を含む有効期限出力を含むオファー有効期限取引記録に署名し第一当事者に送信する。

【００８７】

本発明の他の実施形態では、取引当事者は第三者が紛争の調停役として行動することに同意する。たとえば、ファシリテータが利用できなくなった場合、払い戻しを呼び出すことを選択するのではなく、一方の当事者が　利用できないファシリテータの代わり仲裁人が間に立つ紛争を引き起こす。　コミット取引のコミット出力の条件は、第一当事者、第二当事者、ファシリテータ、およびメディエータのうちの二人の承認を必要とする。有効期限タイムスタンプ時または条件によって定義された時点であり完了払い戻し取引記録のロックタイムの前に、紛争当事者と仲介者はそれぞれ署名し、一方の当事者は第一の当事者、第二の当事者、およびメディエータのうちの二人の承認を必要とする条件及び紛争出力を含む紛争取引記録を提出する。紛争が解決されると、当事者の署名、または仲介者と当事者の一方が、上記の支払い取引記録と同様の決済取引記録に署名するが、それは仲介された和解を反映する。

【００８８】

図１５から図１６は、そのような二つの実施形態の態様を示す。図１５の紛争取引はファシリテータの手数料の金額（ϕ_X）を含む第一手数料出力とメディエータ手数料の金額（ϕ_M）を含む第二手数料、当事者間で共有される手数料出力、紛争を開始した当事者（Ｂ）が払うメディエータ手数料を含む和解取引から構成される。図１６に示すように、紛争取引は当事者間で共有されるファシリテータ料金を含み、和解取引は紛争を開始した当事者（Ｂ）によって支払われるメディエータ料金を含む。別の実施形態では、任意のメディエータ料金が和解条件として決定され決済取引に含まれる。

【００８９】

任意選択で（そして好ましくは）当事者は、上記と同様の紛争払い戻し取引記録を署名し、送信し、代わりに紛争取引からの入力を取って、和解に至るための十分なロックタイムを設定する。このようにすればメディエータが利用できなくなった場合、当事者は紛争払い戻し取引記録を再度提出することができる。別の実施形態では、紛争処理は「仲介可能」であり、例えば仲介人が利用できなくなった場合に第二の仲介人を命名するなどの紛争の連鎖を可能にすることができ、払い戻し取引記録のロックタイムが近づいている場合仲裁人がロックタイムを延長するなどできる。

【００９０】

他の実施形態では、調停を自動化することができる。　例えば、スワップまたは同様の取引に関連する実施形態では、署名されていない支払い取引記録が作成された時点で取引が停止されたかのように、ファシリテータは署名されていない支払い取引記録を定期的に取引者に送信する。署名されていない支払い取引は、それが作成された検証可能な時間、またはそのような時間への参照を含む（例えば、転送メカニズムがビットコインまたは同様のプロトコルであり、スクリプトの一つに埋め込まれた未使用の署名データファシリテータが所有する別個の鍵であり、入力の署名には使用されないなど）。　当事者に送信したり、署名された支払い取引記録を提出したり、有効期限を過ぎても利用できなくなったりする前にファシリテータが利用できなくなると、紛争が開始され、当事者間で条件及びファシリテータからメディエータに受け取った署名されていない支払い取引記録の一部またはすべてを交換する期間がある。（各当事者によって署名されることが好ましいが、当事者が同意する場合、すなわち同じ条件をメディエータに送信する場合は不要である）。メディエータは、両当事者から受領した署名のないまたは署名された条件、および確認可能なすべての署名されていない支払い取引記録を調べる。他の一実施形態では、メディエータは、最新の検証可能な署名されていない支払い取引記録を選択するだけである。別の実施形態では、仲介者は、署名されていない支払い取引記録を順番に「再生」し、署名されていない支払い記録が取引の初期終了を引き起こしたはずであるかどうかを検証する（例えば、一方の当事者の元本および担保が枯渇した場合）。さらに別の実施形態では、メディエータは、一つまたは複数のデータソースからの情報を要求し、独立した条件の評価

をファシリテータの代わりに実行する。これは、支払い取引記録にできるだけ近い新しい若い取引が作れるようメディエータが決定できるように、ファシリテータによって作成される。

【００９１】

図示の実施形態は、本発明のより基本的なものであることに留意されたい。ソース取引、コミット取引、支払い取引、払い戻し取引、有効期限取引、入力、出力、および、元本、担保または料金のさまざまな組み合わせは、参加間の契約によってのみ制限され、本発明により有効になる　。　さらに、本出願を通して開示される実施形態の特定のステップは、特定のエンティティによって実行されるものとして説明される。　他の実施形態では、本明細書に記載されたものの代わりに、またはそれに加えて、同様または同等のステップを、全部または部分的に、異なる当事者によって実施することができる。そのような実施形態の全ては、本発明の範囲内にあると考えられる。

【００９２】

非常に簡単な例として、分散型デジタル通貨を使用する実施形態では、取引はマルチシグナリング取引の代わりにＰ２ＳＨを使用している。特定の実施形態では、他のステップを省略することができる。例えば、分散型デジタル通貨を使用する実施形態では、署名された完了払い戻しまたは失効取引記録の作成は、ファシリテータまたは相手側が消滅するか非協力的になる場合の損失を避けるための対処法として強く推奨されるが、それは厳密に必要ではない。メディエータを含む本発明の実施形態では署名されていない紛争処理記録は、ファシリテータによって作成され、例えば払い戻し取引または有効期限取引記録が作成されて送信されるときにメディエータと共に使用するために当事者に送信される。

【００９３】

図１７から図２２は、ブロックチェーンを含む分散型デジタル通貨を含む転送メカニズムを使用して、一実施形態内のスワップの形で値転送を行う主要な段階を示す図である。図１７、１８は第一段階を示し、クライアントは、ファシリテータとの第一の注文（基本証券、見積もり証券、元本、担保、支払い機能、有効期限タイムスタンプ等）を含む第一の注文を確認する。　クライアントは、第一の元本取引を作成するために、その条件に適合する第一の元本取引記録を転送メカニズムに提出（ブロードキャスト）する。ファシリテータは、更新のブロックチェーンを監視し、第一の元本取引が確認されたときに第一の注文を活性化する。図１９は、ファシリテータが第一注文を第二注文と照合し、コミット取引記録を作成して転送メカニズムに提出（ブロードキャスト）してコミットを生成することによって第一元本取引および第二元本取引からの出力をコミットする第二段階を示す。任意選択で、ファシリテータは、コミット取引からの出力を費やし、有効期限のタイムスタンプの後まで使用することができない払い戻しまたは「ロールバック」取引記録を作成して各クライアントに提供する。　ファシリテータが壊滅的に失敗した場合、どちらのクライアントも署名して払い戻し取引記録を提出して、両方のクライアントを元のそれぞれの立場に戻すこともできる。図２０は、第三段階を示しており、ファシリテータは、データソースから１つ以上の値を受け取り、その値、元本、および担保に支払い機能を適用して評価を監視して、一方の当事者の元本、および担保は枯渇しているかを調べる。任意選択で、各クライアントは、ファシリテータから状況の更新を受け取り、ファシリテータのステータス更新をデータソースから１つ以上の値を独立して受信する。また、図２１－２２は、有効期限タイムスタンプの後に（またはいずれかの当事者の元本および担保が枯渇した場合、いずれか早い時点で）、ファシリテータはコミット取引の出力を費やす１つまたは複数の支払い額を含む、一つ以上の支払い出力を備えた未完了支払い取引記録を作成する。いずれかのクライアントが完了支払い取引記録を受信し、それを完了（サイン）して、完了支払い取引記録を作成する。　クライアントは、支払い取引を作成するために、転送取引に完了支払い取引記録を提出（ブロードキャスト）し、クライアントの両方の資金を同時に解放する。

【００９４】

図２３は、クライアント（１２０）またはファシリテータ（１００）を含む典型的な実

施形態の構成要素を示す。これは、メモリ（１７０）およびネットワークインターフェース（１９０）に結合されたコンピュータプロセッサ（１６０）を備える。コンピュータプロセッサ（１６０）は、図示のような単一の処理ユニットに限定されず、当技術分野で知られているように、複数のコア、複数のコンピュータプロセッサ、ネットワーク化されたコンピューティングデバイスのクラスタ、メモリ（１７０）などを持つ。メモリもハードディスクに限定されるものではなく、ファイルのデータが別個の論理セクタ（１８０）に格納されることを可能にする固定メモリ技術を持ち（例えば、一つ以上の論理ファイルを含むことができるシステム内の一つ以上の論理記録、ファイルまたはデータベース内の一つ以上の論理記録など）、およびコンピュータプロセッサへの電力供給が中断された場合にデータが持続することができる。ソリッドステートストレージ、フラッシュドライブ、ＲＡＩＤ、ＪＢＯＤ、ＮＡ８、ＡｍａｚｏｎのＳ３のようなリモートストレージサービスやＧｏｏｇｌｅのクラウドストレージ、メモリのクラスタデバイスなどは当技術分野で知られているような組み合わせの例だが、それのみにとどまらない。クライアント（１２０）の場合、メモリ（１７０）は、非対称キーペア（２００）を保管するための１つまたは複数のキーペアセクタを含む一つ以上の論理セクタを備える。　ファシリテータ（１００）の場合には、メモリ（１７０）は、一つ以上の鍵ペアのセクタ（２００）ならびに１つまたは複数の取引記録を格納するための一つ以上の取引記録のセクタを含む一つ以上の論理セクタを含む。ネットワークインターフェース（１９０）は、図示のように単一のネットワークインターフェースに限定されない。ネットワークインターフェースには、当技術分野で知られているロードバランサ、２つ以上の多重化ネットワークインターフェースなどがあるがそれだけには限定されず、またはそれらの組み合わせを任意に含む複数のネットワークインターフェースを備えることができる。

【００９５】

図２４（先行技術）は、分散型デジタル通貨での所有権の単純化された繋がりを示しているが、実際には、取引は複数の入力および複数の出力を有することができる。

【産業上の利用可能性】

【００９６】

本発明は、所有権の移転を考慮する別個の当事者間の合意、ならびにこの発明が価値、重要性をもちうるあらゆる産業に関連する。

【００９７】

用語の説明

これらは便宜上提供される用語の簡単な説明である。定義を限定することを意図するものではなく、当技術分野で理解されているか、または本明細書の他の箇所に記載されている任意の特徴、特性、挙動、実施形態を補足するものである。

【００９８】

「クライアント」（１２０）：コンピュータプロセッサ（１６０）と、ペアキーのセクタ（２００）を有するメモリ（１７０）を含む非対称キーペアを保管するための装置であり、ネットワークインターフェース（１９０）、およびその本発明による転送メカニズム（１１０）を介した価値転送を容易にするための、他のクライアント（１２０，１７０）かファシリテータ（１００）の少なくとも１つと相互作用するように構成されている。

【００９９】

仮想通貨は、「分散型デジタル通貨」を参照。

【０１００】

「分散型デジタル通貨」（１５０）：取引の分配元帳を含む転送メカニズム（１１０）（ビットコインプロトコルおよび子孫など。「ブロックチェーン」と呼ばれることが多い）典型的には一人以上のマイナーを含む一つ以上のネットワークネットワーク参加者を含む。「仮想通貨」とも呼ばれる。

【０１０１】

「ファシリテータ」（１００）：第一のクライアント（１２０，１６０）を利用する第一当事者と、第二のクライアント（１２０，１７０）を利用する第二の当事者との間で転

送メカニズム（１１０）を介して価値転送を容易にするための装置（１１０）であって、本発明によれば、装置はコンピュータプロセッサ（１６０）と、取引記録セクタと、非対称キーペアを記憶するためのキーペアセクタ（２００）と、ネットワークインターフェース（１９０）を含むメモリ（１７０）を備える。

【０１０２】

「証券」：あらゆる種類の価値のある取引可能なもの。現金、事業体に対する所有持分の証拠、または現金その他の金融商品を受領または提供する契約上の権利のいずれかである。「金融商品」とも呼ばれる。国際財務報告基準によれば、「ある企業の金融資産と他の企業の金融負債または持分証券を生じる契約」である。

【０１０３】

「ロックタイム」：タイムスタンプが経過するまで、取引が転送メカニズムによって有効であると受け入れられないようにする日付と時刻、任意選択でタイムゾーンを含むタイムスタンプ。

【０１０４】

「当事者」：所有権を行使することができる法人。例えば、個人または法人。

【０１０５】

「［デバイス］に取引記録を公開する」：デバイスによる読み取りやコピーのために利用可能な取引記録の作成をすることであり、例えば、ネットワークインターフェース（１９０）を介してデバイスへの取引・記録を送信すること、または必要に応じてデバイスの読み取りまたはコピーできるように取引記録を書き込むこと、任意選択で取引記録を読み取り及びコピーができるが作成、更新、破壊はできないスキームの認証を実装することなど。非限定的な例には、共有ファイルシステム（例えば、ＮＦＳ、ＳＳＨＦＳなど）、データベースＡＰＩ（例えば、ＳＱＬ、ＲＥＳＴなど）、専用ＡＰＩ、第三者共有ストレージ（例えば、Ｇｏｏｇｌｅ　Ｄｏｃｓ、Ｄｒｏｐｂｏｘ、等）などがある。

【０１０６】

「取引記録を［転送メカニズム（１１０）］に提出する」：有効な取引記録が取引を実行するために転送メカニズム（１１０）によって受け入れられるプロセスを指す。分散デジタル通貨（１５０）の文脈では、典型的には、ネットワーク参加者の過半数によって有効と認められている有効なブロックに取引記録を含む一人以上のマイナーによって受け入れられた取引記録を有する一人以上のネットワーク参加者に取引記録をブロードキャストすることを含む。分散型デジタル通貨（１５０）の文脈では、多数のネットワーク参加者によって有効とされる取引の受け入れは、永久的かつ不可逆的である（例えば、すでに使用済みのアウトプットを費やそうとしたことなどが後で大部分のネットワーク参加者によってため判明したため取引記録が無効となるなど）

【０１０７】

「取引」：資産の所有権または管理を（時には特定の条件に基づいて）再特徴付けする移転メカニズム（１１０）における価値転送の単位。分散型デジタル通貨（１５０）の文脈では、これは時々、ネットワーク参加者の大多数台帳またはブロック鎖に承認された取引記録を意味する「確認済みの取引」と呼ばれる。

【０１０８】

「取引記録」：取引を記述するデータ構造であり、取引を実行するために転送メカニズムに提出される。非限定的な例として、分散型デジタル通貨の文脈では、取引記録は典型的には、一つ以上の入力（特別な場合にゼロ入力が可能である）一つ以上の出力、および任意選択で暗号署名を含む。分散型デジタル通貨（１５０）の文脈ではこれは（時に間違って）「取引」とも呼ばれる。あいまいさを避けるため、この仕様では、ネットワーク参加者間で送受信できるデータ構造を参照するために「取引記録」を使用し、取引記録を含むブロックチェーン内の元帳またはブロックの一部を参照する「取引」を使用して、帳簿またはブロックは、ネットワーク参加者の過半数（すなわち、「確認済み取引」）によって有効であると受け入れられる。

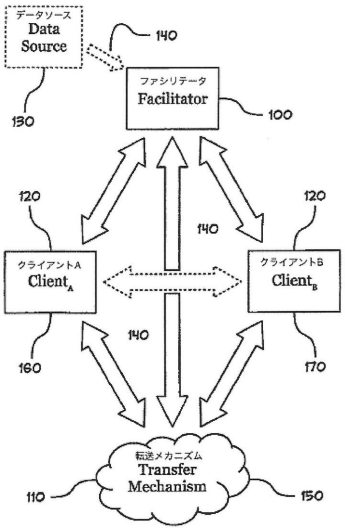
【０１０９】

「転送メカニズム」（１１０）：取引（例えば成功した取引記録の提出など）が作成され強制される手段（例えば分散型デジタル通貨など）

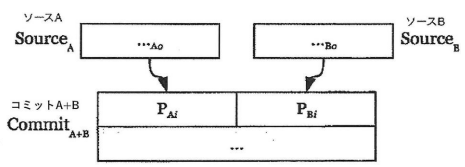
【０１１０】

「価値転送」：当事者の間で経済的な価値を有する物（金、物品、サービス、実行する義務など）の（所有権、制御などの）権利を転送するプロセスである。

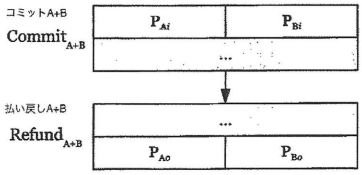
【図１】



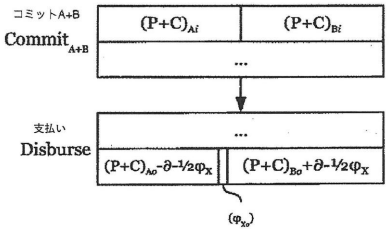
【図２】



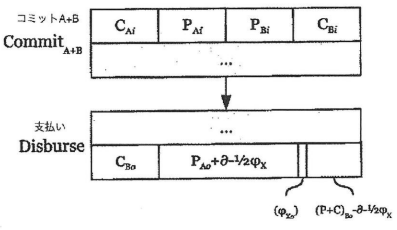
【図３】



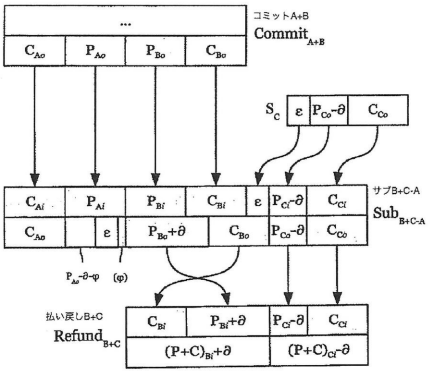
【図４】



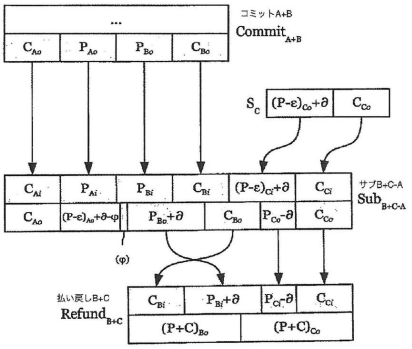
【図５】



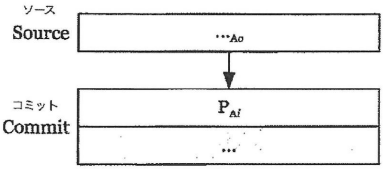
【図６】



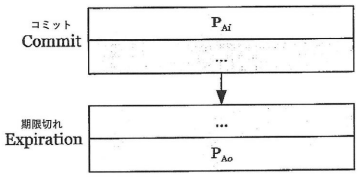
【図７】



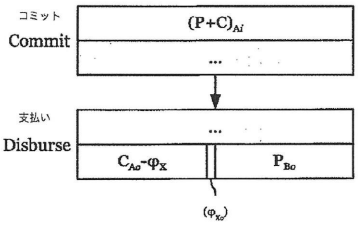
【図８】



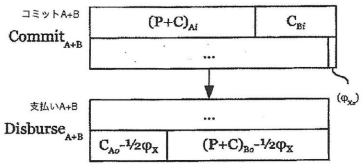
【図９】



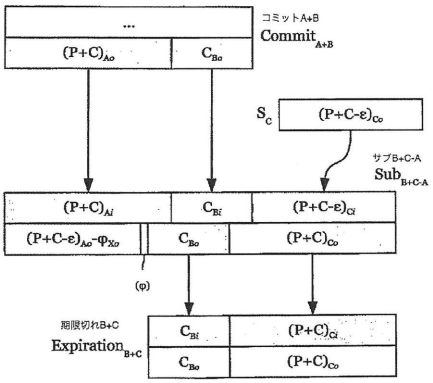
【図１０】



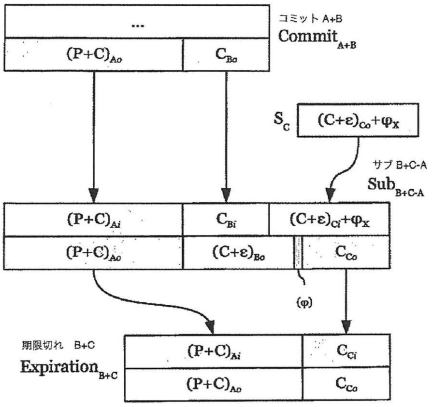
【図１１】



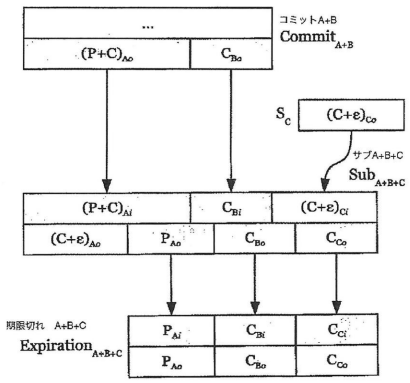
【図１２】



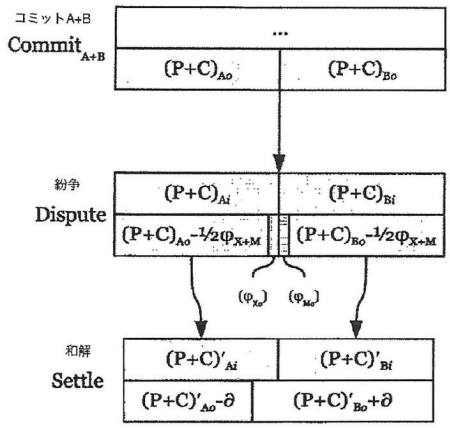
【図１３】



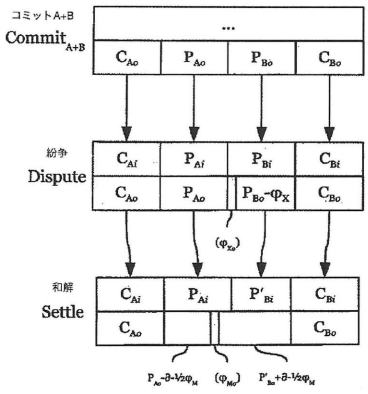
【図１４】



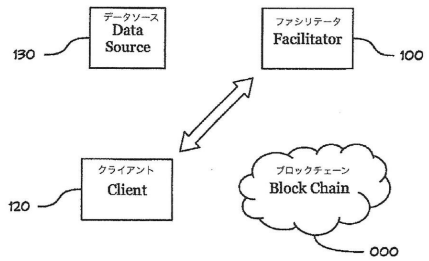
【図１５】



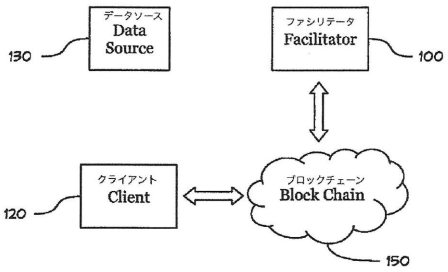
【図１６】



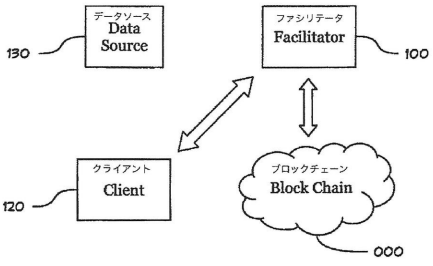
【図１７】



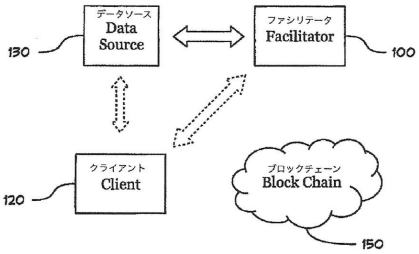
【図１８】



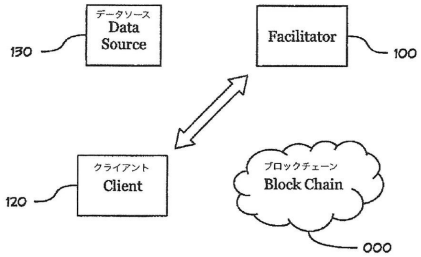
【図１９】



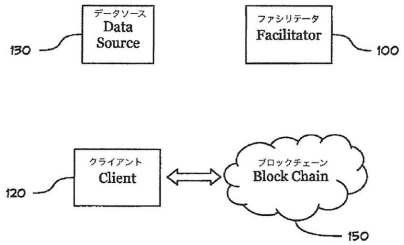
【図２０】



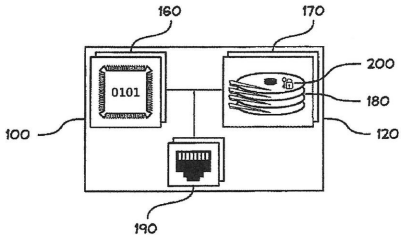
【図２１】



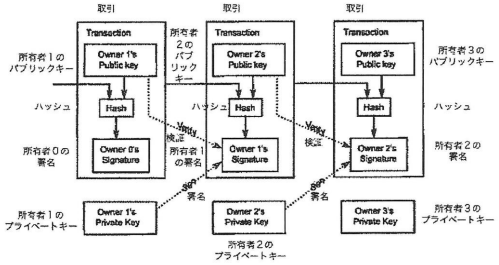
【図２２】



【図２３】



【図２４】



フロントページの続き

審査官　関　博文

(56)参考文献　特開２００２－２３０４４８（ＪＰ，Ａ）
特開平０６－１６２０５９（ＪＰ，Ａ）
米国特許第０７５４６２７５（ＵＳ，Ｂ１）
国際公開第２０１３／１２７７１３（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　　１０／００－９９／００